Sous la direction de

Céline Marangé et Maud Quessard

LES GUERRES DE L'INFORMATION

à l'ère numérique

puf

Sous la direction de
Céline Marangé et Maud Quessard

Les guerres de l'information à l'ère numérique

Ouvrage publié avec le concours de l'Institut de Recherche stratégique de l'École militaire

puf

ISBN 978-2-13-082244-8

Dépôt légal – 1re édition : 2021, janvier

© Presses Universitaires de France / Humensis, 2021

170 bis, boulevard du Montparnasse, 75014 Paris

Ce document numérique a été réalisé par Nord Compo.

PRÉFACE

Jean-Baptiste Jeangène Vilmer

Les manipulations de l'information, qui ont toujours existé, sont aujourd'hui à la fois plus nombreuses et plus graves car elles sont véhiculées par des réseaux sociaux qui permettent de toucher des millions de personnes dans le monde en quelques minutes seulement, dans un climat de crise de confiance dans lequel la parole publique est dévaluée et la notion même de vérité est remise en cause. La pandémie de Covid-19 en 2020 l'a encore illustré : entre fin janvier et fin mars, le Service européen d'action extérieure de l'Union européenne a identifié plus de 150 informations fausses ou biaisées ainsi que des théories conspirationnistes, attribuées à la Russie, sur l'origine du virus, la réalité de la pandémie, les traitements potentiels ou encore les mesures prises par les États. La Chine, où le virus est apparu, est également responsable d'une campagne de désinformation visant à déresponsabiliser le Parti communiste chinois en accusant les États-Unis. Ces attaques ne sont pas anodines : dans une crise sanitaire comme celle-ci, « la désinformation peut tuer » comme l'a rappelé Josep Borrell, le haut représentant de l'Union pour les affaires étrangères et la politique de sécurité.

Ce problème est universel – il se manifeste dans le monde entier, avec ses variantes et spécificités locales – et quotidien, c'est-à-dire qu'il n'est

pas limité aux situations exceptionnelles qui l'exacerbent comme une crise sanitaire, une campagne électorale ou un conflit armé. Il menace particulièrement les démocraties, parce que l'information y circule librement. Il est donc important de l'étudier pour comprendre ses mécanismes, ses acteurs et les tactiques employées, et trouver les meilleurs moyens d'y résister. L'Institut de recherche stratégique de l'École militaire (IRSEM) s'y emploie.

Cet ouvrage, dirigé par deux chercheuses de l'IRSEM[1] et auquel de nombreux autres collègues ont contribué, s'inscrit dans des efforts entrepris depuis 2017-2018 pour faire de notre institut l'un des acteurs majeurs de l'étude des manipulations de l'information. En quelques années, nous avons produit sur ce thème trois rapports, dont le premier, préparé avec nos collègues du Centre d'analyse, de prévision et de stratégie (CAPS) du Quai d'Orsay et lancé en présence de la ministre des Armées en 2018, a contribué à façonner le débat en France et est régulièrement cité à l'étranger ; ainsi que plusieurs autres publications dans nos collections ou à l'extérieur. Nous avons organisé des séminaires réguliers, reçu de nombreuses délégations étrangères et accompli des missions partout dans le monde. Les recrutements en 2017 de Maud Quessard, maître de conférences des universités et spécialiste de la diplomatie publique américaine, ainsi que de François Delerue, juriste spécialiste de cyberdéfense, et en 2019 de Paul Charon, ancien analyste du renseignement spécialiste de la Chine, sont venus nourrir cette ambition, en complétant le travail déjà accompli par Céline Marangé sur la Russie. Ensemble, nous avons développé une expertise encore trop rare dans le monde francophone, comme en témoigne le fait que ce livre est le premier de ce genre.

Il faut louer le travail remarquable accompli par les deux directrices de cet ouvrage collectif, Céline Marangé et Maud Quessard, et le rôle que François Delerue a également joué dès l'origine du projet. Ils ont réussi dans des délais relativement contraints à réunir les contributions d'une

vingtaine d’auteurs, français et étrangers, reconnus pour leur compétence, dans un format à la fois riche et pratique. Ouvrage de référence, clair et accessible, il saura intéresser à la fois le grand public et les chercheurs, étudiants et praticiens de ce domaine en plein développement, qui présente – il faut bien le reconnaître – une certaine confusion terminologique. De quoi parle-t-on ? De *fake news*, de « désinformation », de « propagande », de « post-vérité », voire d’« influence » ou d’« ingérence » ? En 2018, nous avions défendu l’expression « manipulations de l’information », qui s’est rapidement imposée dans le discours officiel français – le projet de loi « anti-*fake news* » puis « contre les fausses informations » ayant été renommé dans ce sens – et est depuis reprise de manière croissante à l’étranger, notamment en anglais.

L’expression que les directrices du présent ouvrage ont choisi de mettre en avant est celle de « guerre de l’information », ce qui se justifie dans la mesure où c’est celle que les Russes (информационная война) et les Américains (*information warfare*) utilisent. En Chine également, ce domaine s’inscrit dans la doctrine militaire dite des « Trois guerres » (*sanzhan* 三战) qui relève de la catégorie plus large de la « guerre politique ». Cette militarisation du champ informationnel, naturelle puisqu’elle renvoie à l’utilisation de l’information comme d’une arme, présente toutefois un risque : celui de donner l’impression que ces opérations informationnelles sont limitées au temps de guerre. Non seulement ce serait vague, puisque la guerre ne fait l’objet d’aucune définition consensuelle, mais c’est exactement le contraire : ces opérations informationnelles font partie des menaces hybrides qui contribuent à établir un continuum entre la guerre et la paix, remettant en cause la pertinence de cette dichotomie. Elles ont lieu tous les jours, tirant profit des zones grises, et leurs acteurs sont autant des États que des acteurs non étatiques, agissant comme leurs proxies ou de leur propre initiative.

Cet ouvrage présente ces « guerres de l'information » dans toute leur diversité, dans le temps (héritage de la guerre froide) comme dans l'espace, en explorant les pratiques des régimes autoritaires (Russie, Chine, Corée du Nord, Iran, monarchies du Golfe) et les réactions immunitaires des démocraties (Royaume-Uni, États-Unis, Israël, Japon, France). Il n'oublie pas non plus les enjeux thématiques, de la réception aux élections en passant par le cyber, la coopération internationale et le rôle de la société civile. Pour traiter les différents aspects de ce vaste panorama, ce livre adopte une approche globale et pluridisciplinaire, qui est nécessaire à l'étude d'un objet par nature transversal. Fort de ces nombreuses qualités, il devrait rapidement s'imposer comme un outil indispensable à la compréhension de l'un des plus graves défis auxquels nos démocraties sont confrontées.

INTRODUCTION

Le nouvel âge des guerres de l’information

Céline Marangé et Maud Quessard

La pandémie du coronavirus de 2020 a suscité des phénomènes d’emballement médiatique et démontré l’extrême viralité de la désinformation en période de crise aiguë. Des réseaux sociaux comme Twitter, YouTube ou Facebook sont devenus le réceptacle d’informations mensongères et le véhicule de rumeurs trompeuses portant sur l’origine de la maladie, l’ampleur du tribut humain ou la recherche d’un vaccin. Relayées par des internautes inquiets et suspicieux, traduites automatiquement par des logiciels de traduction, ces fausses informations se sont répandues à travers le monde, discréditant les pouvoirs publics et entamant la confiance des citoyens dans une période d’épreuve requérant la concorde nationale et la solidarité de tous. La gestion de l’information est apparue aux gouvernants comme un enjeu de sécurité nationale et comme un problème de réputation internationale. Des semaines durant, fausses informations et démentis officiels se sont succédé dans les fils d’actualité, les autorités politiques préférant ne pas laisser sans réponse des campagnes de désinformation orchestrées par les médias d’État de puissances rivales et

reprises en boucle par des groupes et des individus s'appropriant et transmettant leurs contenus non vérifiés.

L'ère de l'information – une expression associée aux années 1980 – s'est caractérisée par l'avènement de nouvelles technologies de communication, telles que le câble et le satellite, qui permettaient une large circulation des images et qui favorisaient déjà des phénomènes de contagion médiatique. Les années 1990 ont marqué le passage à l'ère numérique avec la création de l'Internet commercial en 1996 et la généralisation des ordinateurs personnels.

Mais la véritable mutation est intervenue dans les années 2000, quand sont apparus des machines connectées et des logiciels participatifs. Des plateformes, comme Facebook en 2004 et Twitter en 2006, ont entraîné le basculement de l'Internet 1.0 vers l'Internet 2.0 qui repose sur la mise en relation des utilisateurs. Depuis l'émergence des réseaux sociaux, des médias numériques et des messageries instantanées, non seulement l'information est globale et immédiate, mais les barrières entre les producteurs et les consommateurs d'information tendent à s'estomper. Le statut même de l'utilisateur a changé : de simple récepteur, il est devenu acteur puisqu'il dispose désormais des moyens de choisir ses sources d'information et surtout de produire et de partager de nouveaux contenus[1].

En transformant et en décuplant les capacités de communication, la révolution numérique bouleverse les rapports que les États entretiennent à la fois avec leur société et entre eux, et provoque une rupture semblable à celle de l'invention de l'imprimerie par Gutenberg. Les partisans de la mondialisation ont tout d'abord cru que les outils numériques contribueraient à la démocratisation des savoirs et à la diffusion du modèle libéral. Force est de constater aujourd'hui que la vitesse de propagation de l'information crée des vulnérabilités nouvelles et offre des armes à qui veut attenter à la souveraineté des États et aux institutions démocratiques.

Les guerres de l'information ne sont certes pas nouvelles, pas plus qu'elles ne sont l'apanage des régimes autoritaires. Mais au XXIe siècle plus qu'auparavant, la puissance se fonde sur le contrôle de l'information et sur le pouvoir discursif des États[2]. L'étude des guerres de l'information à l'ère numérique permet de comprendre comment des États, qu'ils soient démocratiques ou autoritaires, affirment leur primauté dans ce domaine et redessinent, ce faisant, les équilibres de pouvoir sur la scène internationale.

L'arme de l'information comme héritage de la guerre froide

Les techniques informationnelles utilisées pendant la guerre froide servent souvent de référentiels dans le débat public. En réponse aux manœuvres médiatiques et cybernétiques de la Russie lors des élections présidentielles américaines de 2016, le général James Clapper, ancien directeur des services américains de renseignement, a ainsi appelé à reconstituer « la machine de l'information de guerre froide[3] ». La confrontation entre l'Union soviétique et les États-Unis continue de façonner les perceptions des dirigeants politiques et le *modus operandi* des exécutants.

Avant de s'interroger sur les ruptures induites par le passage à l'ère numérique, sans doute faut-il rappeler les principales caractéristiques de la guerre de l'information pendant la guerre froide. La compétition des modèles idéologiques a structuré l'antagonisme entre les deux superpuissances. De ce fait, la propagande a été une arme privilégiée, visant, de part et d'autre, à influencer et à persuader. La guerre psychologique a donné lieu à des opérations de désinformation et

d’intimidation. Quant à la subversion, elle a servi à induire en erreur les dirigeants et à déstabiliser les sociétés.

La propagande de guerre comme matrice initiale

Dès leur prise de pouvoir en octobre 1917, les dirigeants bolcheviques revendiquent des opérations de propagande, notamment en direction des « masses ». Constitutive de l’expérience soviétique, la propagande sert de ferment à la guerre sociale pendant la guerre civile russe (1917-1922) en attisant le ressentiment envers les « ennemis de classe ». Le régime soviétique mène, en parallèle, des opérations d’information et de propagande à destination de l’étranger, en s’appuyant d’abord sur l’appareil du Komintern et sur les partis communistes étrangers.

Sous Staline, la propagande totalitaire assène la ligne officielle, fabrique l’image de l’ennemi ; elle contribue à l’atomisation de la société par l’endoctrinement, puis, pendant la « Grande guerre patriotique », à la mobilisation totale de la population[4]. Après sa mort en 1953, la propagande d’État se poursuit et s’édulcore, vantant les mérites du régime, dénonçant les agissements des ennemis et offrant toujours le modèle d’un « homme nouveau » et d’une société socialiste idéale.

Au contraire, avant la Seconde Guerre mondiale, la démocratie américaine n’a eu recours à la propagande qu’en temps de crise, lors de la Révolution (1765-1783), au cours de la guerre civile (1861-1865) et pendant le premier conflit mondial. Quelques mois après l’attaque japonaise de Pearl Harbor en décembre 1941, l’administration du président Roosevelt (1933-1945) fonde l’Office of War Information (OWI) et le charge de mener des opérations de guerre psychologique afin de démoraliser les troupes adverses par la désinformation, la subversion et le sabotage. Aidé de l’Office of Strategic Services (OSS), l’ancêtre de la CIA, l’OWI crée des unités mobiles de propagande à proximité des lignes de front dans le but

d’inciter les soldats allemands et italiens à se rendre[5]. Il se dote aussi d’une radio, la Voix de l’Amérique (VOA), qui fait connaître les positions américaines dans l’Europe occupée, puis libérée[6], et qui développe par la suite des programmes d’information et des activités de diplomatie culturelle.

La diplomatie publique et la guerre psychologique

Au lendemain de la Seconde Guerre mondiale, l’administration du président Truman (1945-1953) ne parvient pas à convaincre le Congrès américain de maintenir des activités de propagande, perçues comme étant incompatibles avec les institutions démocratiques. Toutefois, les autorités américaines adaptent le vocabulaire officiel afin de poursuivre des opérations qu’elles jugent utiles en temps de guerre froide. Fort de son expérience militaire, le président Eisenhower (1953-1961) estime que le facteur psychologique (P-factor) est déterminant pour remporter la lutte idéologique dans la confrontation qui oppose son pays à l’Union soviétique.

Dès son arrivée à la Maison Blanche, il crée l’Agence d’information des États-Unis, connue sous l’acronyme USIA, et lui confie la mission d’influencer des populations étrangères dans le but de promouvoir l’intérêt national américain[7]. L’USIA ne vise pas seulement des populations indifférenciées, mais aussi certains groupes identifiés comme des cibles stratégiques. L’agence développe des programmes qui reposent sur une coopération étroite entre des agences gouvernementales et des institutions privées. Les services d’information des ambassades sont ainsi chargés de vanter le mode de vie américain, en organisant des expositions, des projections de films et des campagnes de publicité[8].

Après le début de la guerre froide, l’Union soviétique intensifie également ses opérations de propagande et d’influence à l’étranger. En 1947, elle met sur pied le Kominform, un bureau d’information des partis

communistes, destiné à uniformiser le discours de politique étrangère des pays de l'Est. Dans les décennies suivantes, divers relais d'influence, comme les partis communistes et le mouvement pour la paix, sont mis à profit dans les pays occidentaux ; des instruments médiatiques, comme la Radio de Moscou et l'agence de presse Tass, font connaître les vues du Kremlin sur les affaires internationales partout dans le monde. Pour contrer l'influence grandissante d'Hollywood et de la culture populaire américaine, les arts et le sport soviétiques, ainsi que la culture littéraire et artistique russe, sont mis à l'honneur, notamment dans le domaine du cinéma, de la musique et de la danse classique.

Le Kremlin et la Maison Blanche cherchent à s'opposer aux actions informationnelles de l'adversaire. Mais si l'expérience du maccarthysme est circonscrite dans le temps, la lutte contre l'influence occidentale demeure un souci permanent des autorités soviétiques. Après sa prise de fonction à la tête du KGB en 1967, Iouri Andropov crée la Cinquième direction du KGB pour combattre « les diversions idéologiques inspirées depuis l'étranger par les opposants » du pouvoir soviétique. Dans une note adressée au Politburo, il souligne l'importance que les États-Unis accordent à la « guerre psychologique » dans la lutte contre le communisme, et affirme la nécessité de « démasquer les intrigues des services secrets et des centres antisoviétiques » opérant à l'étranger et d'éradiquer « les phénomènes malsains dans certaines couches de la population », susceptibles « d'être exploités par l'adversaire à des fins de sape[9] ».

Le rôle de la subversion dans la lutte idéologique

À l'extérieur du pays, les services secrets soviétiques mènent aussi des opérations de subversion afin de déjouer les complots qui seraient ourdis contre leur pays. Dans ses mémoires, le général du KGB Oleg Kalugin cite de larges extraits de la doctrine de renseignement soviétique à la rédaction

de laquelle il a participé dans les années 1970, en tant que directeur du « Département K » chargé du contre-espionnage à l'étranger. D'après ce document, le KGB cherche alors à « se procurer à l'étranger des informations sur les intentions hostiles, les desseins, les formes et les méthodes d'action pratique des services d'espionnage et de contre-espionnage des pays du principal adversaire, les organismes de guerre psychologique et les centres de diversion idéologique ». Il recourt, en plus, à des « mesures actives » (*aktivnye meropriâtiâ*) afin de désinformer les services secrets étrangers sur ses intentions et d'induire en erreur des cibles gouvernementales, politiques et militaires, en particulier dans les moments de crise[10].

Un dictionnaire du contre-espionnage datant de 1972 et classé top secret précise l'étendue des « mesures actives » : elles consistent à créer des réseaux d'« illégaux[11] », à recruter des agents et à acquérir des informations secrètes, mais aussi « à désinformer, compromettre et corrompre les forces de l'adversaire ». L'objectif est « de mettre au jour et d'empêcher une activité hostile au stade le plus précoce de son apparition, à forcer l'adversaire à se découvrir, à lui imposer sa volonté, à le forcer à agir dans des conditions défavorables et dans une direction nécessaire aux services de contre-espionnage[12] ». Concrètement, il s'agit de manipuler des journalistes et des agents d'influence, de diffuser de fausses rumeurs et de fabriquer des faux afin de discréditer les adversaires de l'Union soviétique auprès de l'opinion internationale[13].

Face à ces manœuvres, les États-Unis passent aussi à l'offensive. Confrontée à la multiplication des victoires communistes dans le tiers-monde, l'administration du président Carter (1977-1981) mise sur la promotion des droits de l'homme. Le président Reagan (1981-1989) relance par la suite la lutte idéologique contre l'Union soviétique qu'il qualifie d'« empire du mal ». Pour remporter la guerre des idées, son administration s'appuie sur des stratégies indirectes de déstabilisation des régimes

communistes et soutient toute initiative « permettant à un peuple de choisir sa propre voie[14] ». Cette période de « nouvelle guerre froide » se caractérise par une escalade médiatique et par la fabrication de fausses nouvelles ou de fausses accusations, parfois étayées de fausses preuves[15]. Elle présente un contraste saisissant avec la Perestroïka, qui augure un réchauffement des relations entre les deux blocs. La politique de transparence (*glasnost'*) initiée par Mikhaïl Gorbatchev laisse croire momentanément que le passage d'une « culture du secret » à « une culture de l'information » est possible[16], même si ses effets restent limités.

Après la fin de la guerre froide, les combattants américains de la désinformation (*warriors of disinformation*) sont congédiés, tandis que le dispositif de diplomatie publique américain, jugé obsolète, est absorbé par le département d'État. Leurs homologues russes, abasourdis par l'effondrement de l'Union soviétique, préparent dans l'ombre leur revanche. Les institutions de propagande soviétiques cessent *de facto* d'exister, mais il n'y a pas eu d'*aggiornamento* ou de véritable débat public concernant le rapport au monde et la perception de l'environnement de sécurité.

En somme, le cadre de pensée de la guerre froide ne saurait être ignoré dans la mesure où il détermine, au moins en partie, « la carte mentale[17] » des dirigeants politiques et leur appréhension des guerres de l'information, mais il ne saurait suffire, tant la révolution numérique introduit des bouleversements fondamentaux dans la manière de communiquer.

L'information comme enjeu de sécurité nationale

La révolution numérique du début des années 2000 coïncide avec la perte des illusions sur la victoire des idées libérales après la guerre froide. Les États-Unis ont certes remporté la guerre des idées qu'ils livraient à

l’Union soviétique et dominé, dans les années 1990, la scène internationale, tout autant que l’espace médiatique et culturel mondial, mais ils n’ont pas su faire triompher leur modèle politique dans le monde. Leur leadership n’a cessé de s’éroder depuis les attentats du 11 septembre 2001 et leurs interventions militaires en Irak et en Afghanistan.

L’étiolement de l’hégémonie américaine se manifeste également par une transformation du paysage médiatique mondial et par l’apparition de nouveaux médias de masse. Les États sont plus exposés que par le passé aux influences extérieures en raison de la numérisation des échanges et de la mondialisation de l’économie. Les régimes autoritaires, comme les démocraties libérales, ne perçoivent plus seulement l’information comme un instrument de rayonnement, mais aussi comme une source de vulnérabilité.

La sécuritisation de l’information

À l’ère numérique, la protection des flux d’information et des infrastructures dédiées est devenue un enjeu de sécurité majeur pour tous les dirigeants. Cette question touche à la sécurité nationale dans la mesure où des adversaires extérieurs peuvent mettre en péril la stabilité d’un pays et porter atteinte aux fondements de son système politique en catalysant le mécontentement, en manipulant des informations et en menant des campagnes d’influence.

Le problème est d’autant plus complexe que les autorités se heurtent à des adversaires déclarés, mais aussi à divers acteurs privés, qui accomplissent des activités d’information et de subversion de divers types. Les conseillers en désinformation d’autrefois ont été rejoints par des mercenaires vendant au plus offrant leur savoir-faire en matière de hacking et d’attaques cyber. Ces derniers peuvent intervenir dans le vol de données

et la mise en œuvre de campagnes de désinformation, avec ou sans l'assentiment des autorités de leur pays.

La définition des responsabilités et la coordination des réponses présentent également des défis nouveaux en raison du rôle que les utilisateurs et les opérateurs peuvent jouer dans les opérations de désinformation. D'un côté, les phénomènes d'amplification sur Internet dépendent en grande partie du comportement de certains utilisateurs, qui, à leur insu ou en toute conscience, deviennent des agents actifs des campagnes d'influence ou de désinformation. De l'autre, les grandes multinationales Google, Apple, Facebook, Amazon et Microsoft, connues sous l'acronyme GAFAM, peuvent difficilement être tenues pour responsables des manipulations de l'information dont elles sont le vecteur non intentionnel, en particulier en contexte électoral. L'Union européenne a néanmoins pris des dispositions spécifiques grâce à la directive SRI sur la sécurité des réseaux et de l'information et au règlement européen sur la protection des données afin de responsabiliser les GAFAM.

Face à l'ampleur de ces questions, une méthode de recherche qui consisterait à se concentrer uniquement sur les actions entreprises dans le domaine de l'information et sur les moyens à mobiliser pour sécuriser un espace virtuel, paraît insuffisante. Il faut de surcroît inclure une réflexion sur la construction discursive de la menace et comprendre comment celle-ci s'articule à la politique de gestion de la menace. Le concept de sécuritisation – à ne pas confondre avec celui de sécurisation, qui renvoie à la seule protection – sert à examiner comment un enjeu est transformé en problème de sécurité et pourquoi son appréhension peut s'écarter des circonstances matérielles constatées objectivement[18]. Thierry Balzacq définit la sécuritisation comme un ensemble de processus à travers lesquels un acteur mobilise des ressources discursives (métaphores, stéréotypes, émotions) et non discursives de façon à convaincre son audience cible de la

dangerosité d’un problème et à légitimer les politiques qu’il envisage pour y remédier[19].

Les préventions des régimes autoritaires

Les régimes autoritaires se caractérisent par le refus de tolérer l’expression de désaccords politiques dans la sphère publique et considèrent la libre circulation des idées comme une source majeure de danger. La révolution numérique, qui favorise une diffusion horizontale de l’information et qui renforce l’agentivité des sociétés, a renforcé leurs préventions. Les soulèvements populaires des « printemps arabes » en 2011 ont particulièrement avivé leurs craintes car ils ont démontré la puissance des réseaux sociaux, utilisés à des fins de mobilisation et de ralliement.

De nos jours, la tâche est ardue pour qui veut contrôler l’information, étouffer l’opposition ou empêcher des révélations embarrassantes. Il ne suffit plus d’exercer un contrôle vertical sur les médias d’État en mettant au pas une poignée de journalistes ; il faut en outre freiner l’expression horizontale d’idées alternatives par le biais de sites Internet, de médias sociaux anonymes et de systèmes de cryptage complexe, ce qui pose des obstacles techniques. Certaines messageries, par exemple Telegram, Signal et WhatsApp, proposent une communication de « pair à pair » qui en principe n’est pas déchiffrée par une plateforme centralisée.

Par ailleurs, les révélations d’Edward Snowden en 2013 sur l’ampleur de la surveillance exercée par les services de renseignement américains attisent la méfiance de nombreux dirigeants, notamment en Chine et en Russie. Les nouvelles technologies décuplent les capacités potentielles d’intrusion des autres acteurs de la scène internationale en permettant l’écoute téléphonique des dirigeants, l’interception et la collecte d’informations en ligne, ainsi que l’espionnage de câbles sous-marins et d’équipements informatiques.

En matière d'information, les régimes autoritaires optent généralement pour une posture à la fois défensive et offensive. D'un côté, ils tentent de stopper certains flux d'information en déployant des mesures de confinement, de blocage et de filtrage, et en judiciarisant l'expression de positions jugées hostiles sur Internet. Ils cherchent aussi à protéger leurs infrastructures critiques et à se prémunir contre toute tentative d'espionnage. De l'autre, ils exploitent les leviers d'influence qu'offre la révolution numérique pour porter atteinte à leurs adversaires déclarés dans le champ informationnel. Dans cette confrontation, ils disposent d'un avantage certain puisqu'ils peuvent à la fois manipuler des relais d'opinion avec une efficacité décuplée et subvertir la liberté d'expression qui prévaut dans des sociétés ouvertes.

Les vulnérabilités des régimes démocratiques

La révolution numérique met aussi à rude épreuve les démocraties libérales. Leurs vulnérabilités sont liées à leur degré de développement technologique et au fonctionnement de leur société. Tout d'abord, les opérateurs d'importance vitale, comme les hôpitaux ou les centrales nucléaires, étant hautement connectés, une attaque sur la couche infrastructurelle ou logicielle du cyberespace peut facilement les mettre hors d'état et, par voie de conséquence, menacer la sécurité physique des personnes. Ensuite, l'apparition des réseaux sociaux facilite les mobilisations en ligne et exacerbe la crise de légitimité dont souffrent les élites politiques et gouvernementales. Une campagne de désinformation peut être difficile à contrer dans la mesure où toute interdiction est perçue comme une censure.

Enfin, certains outils numériques font peser une menace sur le jeu démocratique. La collecte et l'analyse des données en ligne permettent de connaître les goûts et inclinations d'une personne, tandis que le traitement

des algorithmes facilite son ciblage. Il est désormais possible d'adapter un message pour mieux manipuler une personne sans qu'il y ait d'intervention humaine directe, comme l'a montré le scandale lié aux activités de la compagnie de communication Cambridge Analytica lors des élections présidentielles américaines de 2016. Tout bien considéré, les guerres de l'information constituent des facteurs d'accélération des évolutions des sociétés démocratiques et mettent à l'épreuve leur capacité de résilience.

Avec l'essor de l'intelligence artificielle, les gouvernements soucieux de préserver les institutions démocratiques et la sincérité du vote se trouvent confrontés à des dilemmes cornéliens, tout autant qu'à des questions insolubles. Les démocraties peuvent-elles, en temps de paix, utiliser « les armes de l'adversaire » sans renier leurs valeurs et dévoyer leurs principes ? L'information du public et l'éducation aux médias suffisent-elles à prémunir les citoyens d'éventuelles manipulations et à garantir la préservation de sociétés ouvertes, alors que la crise de confiance s'accroît, que se développent des faux quasiment indétectables et que se répandent des techniques que l'on appelle *deep fakes* et qui permettent au plus grand nombre de créer facilement des faux ?

La révolution numérique comme rupture stratégique

En plus d'être un enjeu de sécurité, la révolution numérique constitue une rupture stratégique dans la mesure où elle bouleverse à la fois l'ordre international et la chose militaire. Les nouveaux outils numériques permettent, en effet, de concevoir et d'exécuter des opérations de combat suivant des modalités nouvelles, mais aussi de procéder à des opérations

d’influence et de désinformation d’une ampleur et d’une sophistication jusqu’alors inégalées.

Les principales puissances mondiales ne sont donc plus seulement engagées dans une course aux armements, mais aussi dans une course aux technologies de l’information, alors que l’apparition de nouveaux acteurs remet en cause la suprématie technologique occidentale.

Un nouvel espace-temps sur le théâtre d’opérations

Les bouleversements technologiques induits par la révolution numérique ont transformé la conduite des opérations militaires. La transmission instantanée d’images satellitaires permet une meilleure connaissance du terrain. Les moyens de communication améliorent la coordination entre les forces engagées et réduisent les chaînes de commandement et les délais de décision. En 2013, le chef d’état-major russe, le général Guerassimov, dressait un inventaire des principales évolutions sur le champ de bataille :

> Les actions militaires deviennent plus dynamiques, plus actives, et donnent plus de résultats. Les pauses tactiques et opératives[20] dont l’adversaire pourrait tirer profit disparaissent. Les nouvelles technologies de l’information ont permis de réduire de façon significative la rupture entre les troupes et les organes de commandement en termes d’espace, de temps et d’information. […] Les distinctions s’effacent entre les niveaux stratégiques, opératifs et tactiques, et entre les actions offensives et défensives[21].

Les outils numériques ont permis d’optimiser la communication stratégique en opération et de l’intégrer à la planification. La maîtrise des effets sur des groupes cibles représente l’une des principales préoccupations

tactiques des acteurs de terrain, qui distinguent les campagnes à large spectre des opérations à visée réduite (sur des individus ou sur des groupes précis). Les campagnes à large spectre ont pour but de s'assurer le soutien des populations locales ou de groupes cibles, considérés comme des relais d'influence. Elles peuvent échouer en cas de mauvais ciblage. En Afghanistan, les opérations d'influence de l'armée américaine, comme *Enduring Freedom*, étaient inadaptées à l'environnement culturel. Les populations ciblées, souvent illettrées, ayant une culture orale ne recouraient pas aux outils numériques.

La démocratisation de l'accès à l'information et la diffusion des systèmes embarqués, comme les drones, contribuent à niveler la supériorité militaire sur le champ de bataille. Formidables caisses de résonance, les réseaux sociaux donnent à un belligérant peu outillé, inférieur sur le plan capacitaire, les moyens de diffuser ses vidéos et ses messages, de recruter des combattants et d'influencer des audiences cibles. Dans la guerre asymétrique qu'il livrait notamment à plusieurs pays occidentaux, Daech a orchestré des campagnes de propagande et de terreur, publiant des contenus en plusieurs langues sur Internet et tirant profit des réseaux sociaux. Il a réussi à convaincre certaines recrues de commettre des attentats sur le territoire des pays qu'il combattait sur les champs de bataille syrien et irakien[22].

Une saturation de l'espace informationnel

On observe, de plus, une saturation toujours plus grande de l'espace informationnel. Il existe de longue date de grands médias internationaux occidentaux, comme la chaîne française TV5 Monde, créée en 1984. Des pays en compétition stratégique développent des discours alternatifs *via* de nouveaux médias, ce qui donne lieu à une prolifération de messages antagonistes. Ils se dotent de chaînes de télévision, chargées d'éclairer

l’actualité internationale suivant un prisme national et de porter un message à des audiences régionales ou mondiales. RT, la chaîne russe, et CGTN, la chaîne chinoise, cherchent à concurrencer CNN et la BBC. Al-Jazeera, la chaîne qatarie, dispose d’une influence sans pareille dans le monde arabe au point d’inquiéter les Émirats arabes unis et l’Arabie saoudite qui ont créé Al-Arabiya à Dubaï sans connaître le même succès d’audience. Pour relayer ses vues, l’Iran s’appuie sur quatre chaînes internationales d’information et sur des radios diffusées dans de très nombreuses langues, ainsi que sur Al-Manar (Le Minaret), la chaîne satellite du Hezbollah libanais.

L’apparition des réseaux sociaux a transformé la communication institutionnelle et la diplomatie publique. Dans les régimes autoritaires, des relais d’opinion sont chargés d’utiliser Twitter ou Facebook pour transmettre le point de vue officiel ou attaquer les vues d’un adversaire. Dans les sociétés occidentales, pratiquement tous les responsables politiques communiquent sur Internet, au point de noyer parfois les messages officiels. Les dirigeants, les ministères régaliens, les ministres et les représentants de la nation maintiennent une présence sur les réseaux sociaux sans forcément coordonner leur action. Le paroxysme de ces brouillages est atteint par le président Donald Trump, qui a envoyé plus de 11 000 tweets pendant les trois premières années de son mandat présidentiel, se livrant à des joutes verbales sur Twitter avec des adversaires des États-Unis, contredisant d’autres fois les annonces de responsables du département d’État.

Face à la multiplication et à la diversification des flux d’information, il devient difficile pour les utilisateurs de hiérarchiser les informations qui leur parviennent et de s’enquérir de leur origine et de leur véracité. L’exercice est d’autant plus malaisé quand les informations arrivent dans leurs « fils d’actualité » qui sélectionnent automatiquement celles qui sont susceptibles de les intéresser *via* des algorithmes tenant compte de leurs choix antérieurs.

Ce nouveau contexte informationnel, caractérisé par des manipulations de l'information toujours plus sophistiquées et indétectables, participe au développement de conflits hybrides, qui associent des opérations de guerre irrégulière à des opérations conventionnelles. Un État ou un mouvement armé dispose désormais d'un plus large spectre d'actions irrégulières pour affaiblir son adversaire, sur le champ de bataille comme à l'arrière, dans le domaine civil.

La fin de la suprématie technologique américaine

La rupture stratégique induite par la révolution numérique tient aussi à l'ascension de la Chine et d'autres acteurs européens et asiatiques dans le domaine des hautes technologies et des sciences de l'information[23]. En s'affirmant comme une puissance de premier plan, la Chine entame le monopole que les compagnies occidentales, en particulier américaines, ont exercé depuis les années 1990 dans le domaine de l'innovation et des hautes technologies. La vallée de Shenzen constitue désormais un pôle d'attractivité au même titre que la Silicon Valley. Alors que des compagnies européennes comme Ericsson et Nokia étaient à l'origine des standards de quatrième génération (4G) pour les téléphones mobiles, c'est Huawei, une compagnie chinoise, qui a mis au point « la brique technologique » de la 5G permettant l'échange de très gros volumes de données numériques en un temps réduit.

Contrairement à la technologie actuellement déployée (4G), une partie des opérations de la 5G se fait « localement », c'est-à-dire directement sur les appareils de télécommunication comme des antennes, ce qui donne un pouvoir inégalé d'écoute et d'interception. L'avance technologique de la Chine, due au désintérêt initial des compagnies européennes pour la 5G, lui offre un effet de levier et un moyen de pression dans les négociations qu'elle mène actuellement avec d'autres États[24]. Néanmoins, les bases

technologiques de la 5G ayant été construites aux États-Unis et en Europe, la Chine n'est ni l'inventrice ni l'unique détentrice de cette technologie-clé. C'est d'ailleurs un autre pays asiatique, la Corée du Sud, qui a déployé la première un réseau 5G en 2019.

En dernier lieu, les guerres de l'information de l'ère numérique deviennent des guerres pour le contrôle des données. Le développement de l'intelligence artificielle dépend de la capacité à rassembler d'immenses banques de données, puis à créer des algorithmes capables d'affiner le ciblage et de calibrer le message en fonction du destinataire. La puissance d'un État dépend donc désormais aussi de sa capacité à accumuler des données. Les rivalités de puissance ne s'expriment plus seulement à travers la guerre des idées ; une compétition pour le contrôle de la datasphère et une course à l'innovation dans le domaine des techniques de l'information viennent désormais s'y superposer[25]. En atteste, par exemple, le projet *Made in China 2025*, qui affirme l'ambition du président chinois Xi Jinping de voir son pays prendre le leadership dans le domaine technologique.

De cet affrontement, il résulte une nouvelle forme de bipolarité sino-américaine qui s'exprime à travers la concurrence des standards technologiques et met sous tension tant les alliances politiques traditionnelles que les pays soucieux de leur autonomie stratégique[26].

Pour une approche globale des guerres de l'information

Les guerres de l'information à l'ère numérique sont le reflet de la société mondialisée : elles ne connaissent pas les frontières et concernent tous les médias et tous les types de gouvernement. Leur étude ne saurait faire l'économie de l'ensemble de ses composantes techniques,

géographiques, politiques et sociologiques. L'originalité de notre approche est d'offrir un large panorama des guerres de l'information en associant dans un même ouvrage les trois dimensions qui les caractérisent.

La première partie s'intéresse aux procédés techniques des conflits informationnels à l'ère numérique. Elle s'ouvre sur une rétrospective de l'usage de l'arme de l'information dans les conflits armés à travers l'histoire, puis envisage les transformations du ciblage et de la guerre électronique dans la conduite des opérations militaires. Les chapitres suivants exposent le fonctionnement des couches matérielles de l'Internet qui permettent d'espionner ou de neutraliser les communications d'un adversaire, et décrivent les phénomènes d'amplification qui produisent des effets sur la couche haute, dite sémantique, de l'Internet, en accélérant la propagation d'une information. Un focus présente les méthodes d'investigation mises en œuvre pour comprendre la diffusion des *fake news*.

Les parties suivantes s'intéressent aux stratégies des États à travers deux séries d'études de cas. Elles permettent de comparer comment des États autoritaires et démocratiques conçoivent et, le cas échéant, mettent en œuvre les guerres de l'information à l'ère numérique. Chaque chapitre porte sur un État particulier (ou un ensemble constitué de pays, comme les monarchies du Golfe) et suit un même cadre d'analyse. Les auteurs s'emploient à caractériser le poids de la propagande dans l'histoire du pays, ainsi que les menaces de type informationnel et leur origine présumée, d'après les documents de doctrine et les discours publics. Ils apprécient l'importance accordée à l'influence dans la pensée militaire et la pratique diplomatique du pays considéré, en cherchant à établir les fins recherchées et les modes d'action privilégiés. Enfin, ils se penchent sur le rôle des acteurs et des institutions chargés de développer des outils d'influence, d'élaborer les doctrines correspondantes et de définir le ciblage, et s'interrogent sur leur cohérence et leur niveau de coordination.

La dernière partie porte sur les implications politiques des actions d'influence et de désinformation, et sur les réponses juridiques et institutionnelles qui ont été apportées pour tenter de réguler ces nouveaux espaces de conflictualité. Elle commence par une réflexion sur la question de la réception, examinant en quoi les sciences de la communication permettent de caractériser les mécanismes de la désinformation, d'analyser les vecteurs de diffusion des infox, et de mesurer leur impact sur des groupes cibles. Vient ensuite un état des lieux des menaces numériques en période électorale, qui souligne l'importance de former les citoyens à ces risques. S'ensuit un chapitre présentant un panorama de la défense informationnelle sur le plan national et international. Un focus montre comment l'OTAN fait face aux menaces cyber et informationnelles. Un dernier chapitre expose les tentatives de régulation pour contrer les manipulations de l'information en visant les acteurs malintentionnés, les comportements trompeurs et les contenus malveillants.

En offrant un panorama des politiques mises en œuvre dans le domaine de l'information par plusieurs acteurs-clés de la scène internationale, comme la Chine, la Russie, les États-Unis, la Grande-Bretagne, la France et le Japon, mais aussi par des États pivots, comme l'Iran et Israël, et par des États isolés, comme la Corée du Nord et le Qatar, notre étude permet d'établir des comparaisons inédites sur les finalités assignées aux stratégies informationnelles, sur les processus de décision politique, ainsi que sur les acteurs chargés d'élaborer et de mettre en œuvre des opérations d'information. Elle a aussi pour ambition d'apporter des éléments objectifs d'appréciation en confrontant différentes approches disciplinaires et en proposant des pistes de recherche et de réflexion future.

Ce travail vient combler un manque : aucun livre de langue française ne traite des guerres de l'information de manière globale. Dans le monde anglo-saxon, il existe une littérature assez abondante sur les guerres de l'information, appelées *i-wars* pour *information wars*. Généralement

produits par des think tanks américains ou d'anciens acteurs institutionnels, ces travaux se limitent en général à décrire des opérations d'information et à élaborer des stratégies de contre-offensive, tout en occultant le plus souvent les pratiques des démocraties libérales dans le domaine informationnel. Or il apparaît que les régimes autoritaires ne sont pas les seuls à se livrer à des opérations d'information. Sans aller jusqu'à considérer l'information comme une arme de guerre, certains pays démocratiques, notamment les États-Unis, recourent désormais à des actions offensives dans le domaine cybernétique et informationnel.

Comme au temps de la guerre froide, la compétition de puissance donne lieu à des actions d'information à grande échelle, visant la population du pays adverse, mais aussi celle de pays tiers. Certains pays africains, par exemple, se trouvent au cœur de luttes d'influence par médias interposés[27]. La mondialisation et l'instantanéité de l'information bouleversent l'ordre international et transforment la nature de la puissance, qui requiert désormais d'affirmer une supériorité technologique dans le domaine de l'information. En même temps, Internet, dont la principale spécificité est d'être distribué et décentré, confère une autonomie relative aux sociétés et aux individus et leur donne la capacité d'agir sur le monde, de contester les stratégies étatiques et d'influencer le cours des événements.

*

Nous exprimons notre gratitude à tous les auteurs pour la confiance, l'enthousiasme et la souplesse qu'ils ont manifestés au cours de la conception et de la rédaction de l'ouvrage. Nous adressons nos sincères remerciements à notre éditeur, Paul Garapon, qui a accueilli ce projet avec bienveillance, ainsi qu'à Jean-Baptiste Jeangène Vilmer, Jean-Vincent Holeindre et Pierre Razoux, qui ont soutenu sans réserve notre initiative. Nous remercions tout particulièrement Chantal Dukers, éditrice à l'IRSEM,

qui a mis un grand soin à préparer les textes, et Maxime Chervaux, qui a traduit de l’anglais deux chapitres.

I

TECHNIQUES ET USAGES DE L’INFORMATION

CHAPITRE 1

L’arme de l’information dans les conflits armés

Nicolas Mazzucchi

Les récents développements des conflits, que ce soit en zone levantine ou en Europe orientale, ont repositionné la problématique de l’utilisation de l’information à des fins offensives au cœur de l’analyse du fait militaire et guerrier. Sans vouloir accepter trop naïvement l’existence d’une révolution du fait militaire par l’information – ou de l’avènement d’une nouvelle forme de guerre dite « hybride » – on ne peut nier l’importance croissante du domaine informationnel, lequel vient en appui des opérations dans les différents espaces (terre, air, mer, etc.). Celui-ci bénéficie, dans le champ conflictuel comme ailleurs, de l’apport des technologies de l’information et de la communication, aussi bien que de la mutation profonde du cyberespace, visible depuis un peu plus d’une décennie. Cette donnée modifie ainsi profondément les approches militaires traditionnelles de l’information, qui ont déjà subi au cours du XX^{e} siècle de nombreux avatars.

L’appréhension de la guerre de l’information – il serait plus juste de parler de la guerre par l’information – qui se superposerait aux actions militaires doit ainsi être analysée, pour en comprendre les ressorts, mais

également les limites. Les armées qui adressent la question au travers de doctrines dédiées sont loin d'être les seuls utilisateurs de l'arme informationnelle dans les conflits. La capacité des acteurs non étatiques à adopter les codes de la communication numérique ainsi qu'à en appréhender les possibilités ne cesse d'étonner. Les groupes armés non étatiques actuels ont su s'approprier un nouvel outil qui leur offre des possibilités extensives en termes de combat asymétrique.

Face à cette situation nouvelle, les forces armées du monde entier font face à un nouveau défi, celui de l'information numérique. Elles doivent aussi anticiper les développements technologiques et sociologiques futurs. Entre contre-narratif, *strategic communication* et combat du faible au fort, les orientations sont variées.

Invariants historiques et développement des médias

Les différentes incarnations de l'emploi de l'information dans les conflits armés se sont fondées tant sur des évolutions de la pensée stratégique que sur le progrès technologique des médias.

La désinformation, une pratique aussi ancienne que l'histoire

L'emploi de la ruse et de la désinformation est aussi ancien que l'histoire puisque la tromperie et la déception, c'est-à-dire l'opération d'information destinée à tromper l'ennemi, sont présentes dès les premiers textes historiques traitant des conflits. La « vertu » d'Ulysse, la *mêtis*, habituellement traduite comme la « ruse », s'identifie également à cette

capacité à tromper l'ennemi en utilisant l'information. Homère fait ainsi de son héros le premier spécialiste des opérations informationnelles au travers du cheval de Troie. À l'autre bout du globe, Sun Tzu décrit dans *L'Art de la guerre* à de multiples reprises des manœuvres de tromperies destinées à prendre l'avantage tactique au moment de la bataille[1]. Toutefois, tant chez Homère que chez Sun Tzu, les opérations informationnelles ont un but simple : préparer le terrain pour la confrontation physique en donnant un avantage tactique avant la bataille.

Un changement profond se produit à la suite des évolutions de la pensée stratégique qui interviennent après la Révolution française et les conquêtes napoléoniennes. L'apport de Clausewitz est ici déterminant[2]. Le positionnement du moral comme centre de gravité de l'action militaire le conduit à accorder une place prépondérante à l'utilisation de l'information dans les conflits armés. Dans ce contexte, toute action militaire est, par essence, une action sur les perceptions, dans ce cas en utilisant la violence. Sans aller jusqu'à considérer la guerre comme une opération d'information militaire à grande échelle, il est néanmoins possible avec Clausewitz de réévaluer l'importance de l'information comme levier d'action sur le moral, tant des combattants que des décideurs politiques. Si cette question de l'intromission de plus en plus grande de l'information au niveau stratégique est palpable dès la fin du XIX^e^ siècle, c'est au siècle suivant que l'information devient un élément central dans le déroulé complet des conflits, avant, pendant et après les combats.

LA MANIPULATION DANS LES CONFLITS DU XX^E^ SIÈCLE

Au-delà de l'apport conceptuel de Clausewitz, les écrits militaires et les penseurs politiques du XX^e^ siècle permettent de prendre la mesure de la croissance du fait informationnel dans les conflits. La mobilisation totale des sociétés européennes, travaillées par la propagande de leur État, ainsi

que les actions intentées pour démoraliser l'adversaire, comme, par exemple, le largage aérien de tracts au-dessus de Vienne par Gabriele D'Annunzio en juillet 1918, favorisent une massification et une industrialisation des actions informationnelles dans le contexte du premier conflit mondial. De nombreux publicitaires sont ainsi mobilisés, notamment pour les affiches de propagande sur les emprunts nationaux ou les engagements volontaires ; d'autres s'engagent dans le domaine politico-militaire comme Edward Bernays, créateur de la publicité contemporaine[3]. Au niveau militaire, les enseignements de la Première Guerre mondiale et les bouleversements qu'elle entraîne se révèlent cruciaux. Le retour d'expérience sur la Grande Guerre et l'importance accordée à la propagande par les bolcheviques russes après la Révolution de 1917 signalent l'importance des médias et de l'information en général. Les travaux de Carl Schmitt sur la dialectique ami/ennemi, ainsi que sur le rôle du partisan dans la guerre, sont élaborés à cette époque. Même si C. Schmitt ne se réfère jamais directement à la question de la place de l'information dans le combat partisan, celle-ci irrigue en creux la réflexion qu'il développe dans son ouvrage *Théorie du partisan*, en particulier la « dimension de la profondeur », mais aussi le démantèlement des structures sociales ou l'évolution technique, puisque ces domaines sont liés par la question de l'information.

Pendant la Seconde Guerre mondiale, les différentes armées prenant acte de ces développements, ont fait un usage extensif des opérations d'information, en particulier au niveau stratégique. Les opérations soviétiques tant contre les forces allemandes que contre les Japonais font un usage extensif des actions informationnelles, regroupées sous le terme de *maskirovka* ou dissimulation, qui recourt aux opérations d'information sans s'y cantonner exclusivement. Les actions préparatoires au débarquement en Normandie ont en ce sens fait appel à toute la palette des moyens informationnels. Les actions se sont ainsi succédé en termes de déception,

de désinformation et d'intoxication du haut-commandement allemand, tant sur la date, les forces et le lieu du débarquement. Les différentes opérations dédiées à ce grand plan (*Fortitude*, *Bodyguard*) qui sont conduites par des unités spécialisées permettent de leurrer l'adversaire par une action de grande ampleur. C'est à cette époque que les concepts militaires de déception, de manipulation (une action informationnelle destinée à obtenir une action précise de la part de l'ennemi), d'intoxication (une action destinée à paralyser le système de décision ennemi) prennent leur acception militaire actuelle. En outre, pendant la Seconde Guerre mondiale, voient le jour des unités de plus en plus spécialisées dans la gestion de l'information, aussi bien en termes de lutte contre la propagande adverse qu'en termes de conduite des opérations dédiées.

L'enjeu du moral dans les conflits de la guerre froide

La fin de la Seconde Guerre mondiale marque une nouvelle ère dans celle des actions d'information. En effet, la peur de la confrontation nucléaire et les évolutions géopolitiques mondiales mettent un terme aux conflits ouverts entre grandes puissances qui privilégient le conflit indirect. De fait, les combats de la guerre froide opposent, le plus souvent, une force armée régulière issue d'un État puissant à un acteur local étatique ou non, militairement bien plus faible, notamment dans le cadre des mouvements de décolonisation. Dans ce rapport du faible au fort qui rend pratiquement vain tout espoir d'une victoire militaire conventionnelle, les médias jouent un rôle central puisqu'ils permettent de déplacer les actions du simple champ militaire local vers un champ politique mondial. Le principal exemple de ce mode asymétrique est visible au travers des conflits d'Indochine et du Vietnam[4]. La diffusion d'images montrant les effets des bombardements américains, en particulier ceux utilisant des agents défoliants (agent orange) ou des effets incendiaires (napalm) est destinée à imposer l'idée d'une

« guerre juste » de la part des forces communistes. L'offensive du Têt en 1968 est un bon exemple des actions informationnelles des communistes vietnamiens puisqu'elle contribue à renverser le cours de la guerre. Action militairement plus que contestable avec un rapport de pertes d'environ 1 à 5 en défaveur du Nord-Vietnam, elle est surtout une action d'information d'ampleur – ici de l'*agit-prop* avec les images des combats au cœur de Saigon, en particulier pour l'ambassade américaine – destinée à faire prendre conscience à la population américaine de la fragilité de la position des États-Unis dans ce conflit. Les opérations d'information servent ici à créer un nouveau front « arrière » où les armées organisées sont plus fragiles eu égard à la nature même des combats.

Concomitamment à ces événements, les travaux du médiologue canadien Marshall McLuhan apportent un socle théorique au cadre médiatique qui évolue dans les années 1950-1960. La théorie du *village planétaire* offre une grille explicative essentielle à la massification des médias qui a lieu, en particulier par le biais de la télévision. Si McLuhan avait déjà théorisé le passage d'une civilisation dominée par l'écrit – la galaxie Gutenberg – à celle dominée par la radio – la galaxie Marconi –, il poursuit sa théorie dans les années 1960 en prophétisant le passage à une société dominée par un médium quasi planétaire et quasi instantané. Il s'agit donc selon McLuhan de positionner l'évolution – le raccourcissement en réalité – de la dimension espace-temps au cœur de la problématique médiologique. Pour lui, le *village planétaire*, loin d'être l'apaisement des passions, est au contraire le lieu de leur expression maximaliste. La problématique évolue depuis environ une décennie avec l'avènement du véritable *village planétaire*, celui de la communication horizontale permise par le Web 2.0, à savoir l'apparition des réseaux sociaux. Force est de constater que ce nouvel Internet des années 2000 correspond de manière quasi idéale – et forcément dystopique – à la vision de McLuhan sur le lieu d'une nouvelle conflictualité.

Le contrôle de l'information dans les conflits post-guerre froide

Les conflits post-guerre froide, à commencer par la guerre du Golfe, introduisent une nouvelle appréhension de l'information comme outil de la panoplie militaire. Prenant acte des raisons de leur échec au Vietnam, les États-Unis décident de se positionner de manière proactive vis-à-vis de l'information. Alors que le cloisonnement de l'information par les militaires avait amené les journalistes à rechercher une vision alternative dans l'autre camp, la guerre du Golfe marque un changement d'approche. Les unités militaires intègrent alors plus directement des journalistes au service d'une narration contrôlée et organisée. Lors de la guerre de libération du Koweït, ceux-ci insistent sur la cause juste, sur la menace que représente l'armée irakienne présentée comme « 4e armée du monde », sur le danger des armes chimiques ou sur la précision des armes de la coalition. Grâce à une communication stratégique (*stratcom*)[5] efficace vers les publics-cibles occidentaux – trop en un certain sens puisqu'elle conduit à populariser le concept de « guerre zéro mort », les forces de la coalition évitent les erreurs des conflits coloniaux et postcoloniaux de la guerre froide, tout en conservant un ascendant sur le domaine informationnel global.

Grâce à l'arme informationnelle, les mouvements de guérilla ont pu à la fois imposer leur tempo et obtenir une initiative stratégique permettant de déplacer le front des opérations du théâtre militaire vers l'opinion publique. Dans les années 1990 ce mouvement est renversé, du moins tant que les médias sont aisément contrôlables. Les *info-ops* et la *stratcom* visent à empêcher le passage à un mode asymétrique de la part des acteurs opposants. Grâce à l'information, les forces occidentales re-symétrisent le conflit et imposent leur tempo, tant qu'elles conservent l'ascendant *via* la technologie de diffusion et le contrôle des canaux de diffusion. À la faveur du retour d'expérience des conflits d'Irak et de Yougoslavie, différentes doctrines sont mises au point, pour les opérations psychologiques visant à

modifier le moral des combattants ou des populations (*psyops*), pour les opérations informationnelles visant à modifier les perceptions des événements (*info-ops*) et pour la communication stratégique destinées aux « arrières » pour expliquer le conflit et son fonctionnement (*stratcom*).

L’information au cœur des conflits contemporains

Le changement majeur dans le domaine informationnel, incarné par l’avènement du cyberespace dans la vie quotidienne de tout un chacun, a des impacts majeurs sur l’utilisation de l’information dans le domaine militaire, en donnant toujours plus de possibilités aux actions offensives.

Le pouvoir égalisateur du cyberespace

Dans la littérature stratégique, il est souvent fait mention du « pouvoir égalisateur de l’atome ». Cette doctrine – au cœur de la posture de dissuasion française – part du postulat que les dégâts causés par une arme nucléaire sont tels qu’ils « égalisent » les forces des protagonistes, même en cas de déséquilibre flagrant dans les capacités conventionnelles. Cette notion de pouvoir égalisateur peut s’étendre au domaine du cyberespace suivant deux schémas. Le premier concerne les cyberattaques sur les systèmes techniques pour lesquelles la somme des connaissances nécessaires est le plus souvent disponible au niveau soit d’un individu, soit d’une équipe réduite. Le second, complémentaire du précédent, concerne le domaine informationnel.

En effet, la prise de conscience, au cours des années 2000 – en Afghanistan et, surtout, en Irak – de l’importance de la communication numérique dans les conflits armés, a naturellement conduit de nombreux

acteurs à s'intéresser à cette dimension qui s'ajoute à celle de l'affrontement physique. Grâce au cyberespace, vu comme espace de communication à la fois immédiat – ou quasi immédiat – et de portée planétaire, les combattants ont réussi à modifier l'une des dimensions de l'affrontement : l'espace-temps. Les talibans, puis les insurgés irakiens, ont ainsi compris comment, grâce à des moyens limités, il était possible de diffuser des messages et des images de propagande – en particulier des embuscades contre les forces coalisées en Irak – vers une audience mondiale[6]. Il apparaît rapidement impossible en Afghanistan de contrôler la narration du conflit, surtout avec la multiplication de dispositifs de communication à bas coût qui font de chaque insurgé – et de chaque soldat – un acteur potentiel d'une communication incontrôlée.

Dans une logique proprement clausewitzienne d'action sur les perceptions adverses, le cyberespace est une caisse de résonance idéale pour, en même temps, atteindre les perceptions adverses – des combattants mais surtout de la population – tout en renforçant celles des acteurs de son propre camp. Il peut même s'agir, dans les cas les plus emblématiques, d'aboutir à un retournement des perceptions de l'action militaire physique par une stratégie d'information efficace, agissant sur l'ensemble des éléments de la chaîne de diffusion.

Le conflit israélo-libanais de 2006 comme exemple

Un exemple s'impose ici, celui de la guerre de juillet 2006 entre Israël et le Hezbollah. La disproportion des moyens militaires, en particulier après la neutralisation de l'armée libanaise par Tsahal, aurait dû conduire à une rapide victoire politique après la victoire militaire. La suite des événements allait démontrer la rapidité avec laquelle la phase informationnelle des conflits modernes pouvait amener à un basculement total. Particulièrement bien équipé pour un groupe armé non étatique, le Hezbollah continuait la

lutte contre les forces israéliennes au Liban ; il a réussi à remporter quelques succès limités. C'est notamment le cas de l'attaque contre la corvette *Hanit* lancée depuis la terre avec un missile de fabrication iranienne. Si la corvette n'a été que légèrement endommagée, cette attaque a donné lieu à une mise en scène informationnelle gigantesque, qui s'est déroulée au-delà du seul théâtre levantin, grâce à l'utilisation d'images truquées, des réseaux sociaux, des blogs et des passerelles informationnelles mondiales.

Cette contre-offensive complexe qui utilise des éléments physiques et informationnels rappelle l'*agit-prop*, un terme russe formé à partir de la combinaison de l'agitation et de la propagande et désignant une action physique (agitation) dont les effets sont maximisés par une diffusion et une amplification informationnelle (propagande). Les réseaux de solidarité informationnelle du Hezbollah ont été engagés afin d'aboutir à ce double objectif déjà mentionné de conforter les soutiens – sur la « justice » de la cause et le déroulement des opérations – et de démoraliser les adversaires. Le résultat de ces opérations informationnelles a fortement contribué à la défaite stratégique d'Israël durant ce conflit par la mobilisation des opinions publiques au Proche-Orient et au-delà contre l'action israélienne et ses résultats présentés comme « désastreux ». Dans ce contexte, comme souvent, l'expérience du conflit a permis une évolution de la doctrine militaire, en particulier à la suite des travaux de la Commission Winograd. Cette évolution se manifeste, par exemple, par la création de comptes Twitter officiels de Tsahal en français et en espagnol dans le but d'opérer une diffusion plus large de la communication stratégique de l'armée israélienne.

Des doctrines militaires intégrant les opérations d'information

Les années 1960-1970 ont vu se généraliser dans les principales forces armées du monde la vision du domaine des perceptions comme une composante à part entière du théâtre des opérations. L'une des premières initiatives en ce sens a été l'emblématique programme civilo-militaire américain au Vietnam CORDS (*Civil Operations and Revolutionary Development Support*). Il vise alors à donner l'image d'une armée américaine qui certes détruit, mais qui reconstruit ensuite et œuvre pour le Vietnam de demain. Le programme CORDS a servi de matrice, même s'il souffre d'une sous-exposition communicationnelle et de son orientation quasi exclusive vers le théâtre des opérations. Depuis cette époque, les forces armées ont cherché à concilier ces impératifs d'efficacité opérationnelle, de limitation de l'impact physique médiatisable des opérations et de contrôle du domaine informationnel, compris comme un nouveau sous-champ de bataille.

Les différentes armées, en particulier dans l'espace euro-atlantique, ont pris la mesure des besoins en termes d'action informationnelle. Les créations d'unités et de matériels dédiés se sont multipliées ces dernières années pour donner à chaque armée son unité ou centre dédié (CIAE en France, 77th brigade de la British Army, 28e régiment « Pavia » dans l'armée italienne, unité Magan de Tsahal, 193rd SOW de l'US Air Force, etc.) à la conduite d'actions informationnelles et psychologiques militaires. Au-delà des unités, certains matériels ont été conçus pour l'action informationnelle comme l'avion de transmission EC-130J Commando Solo III destiné à la diffusion d'informations radiophoniques et télévisuelles sur théâtre.

Il résulte de ces développements une certaine unification de la vision complexe des opérations d'information au niveau des forces armées de l'OTAN qui s'exprime au travers de l'AJP 3.10[7] et qui découle des canevas de planification de l'Alliance. La conception otanienne est fondée sur une dualité entre l'action sur le territoire national et en territoire ami et l'action sur le théâtre des opérations. Cette dualité de lieux est prise en compte dans

le découpage de l'action militaire en niveaux (stratégique, opératif et tactique) puisque les actions de niveau stratégique, avant tout politiques, visent en priorité le territoire national de la force déployée et les actions de niveau opératif et tactique, le théâtre des opérations lui-même.

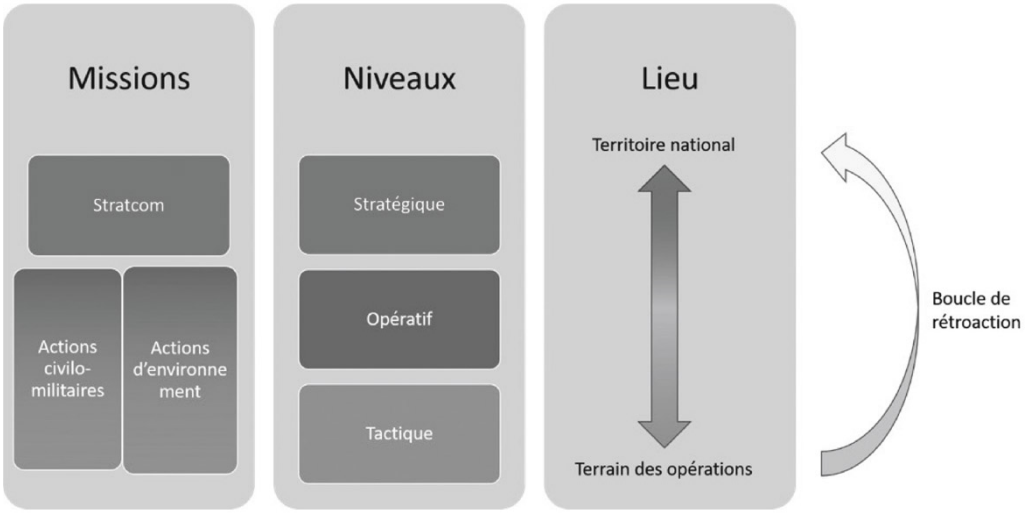
La *stratcom* est en ce sens une action tournée prioritairement vers sa population (et ses décideurs) ainsi que ses alliés. En communiquant sur la cause défendue, la conduite des opérations, les infamies de l'adversaire, il s'agit de renforcer le soutien de sa base, tout en tentant de saper celui de l'autre camp. Opération de temps long et peu agressive, la *stratcom* a pour but premier la mobilisation.

Au niveau du terrain, on constate une fusion prononcée des niveaux opératif et tactique s'agissant des opérations d'information. La plupart du temps, ces dernières sont conduites au niveau tactique, mais avec une prise en compte des effets à l'échelon supérieur. Dans le cas des actions civilo-militaires notamment – lesquelles peuvent se déployer dans le temps très long et par des moyens peu militaires, surtout en phase de reconstruction –, toute mission aura pour but d'agir à la fois sur la réussite de l'action tactique (sécurisation d'une zone géographique donnée, par exemple) mais également sur la perception opérative (amélioration de l'opinion des habitants et décideurs politiques nationaux vis-à-vis des forces déployées).

Il en va de même en ce qui concerne les actions d'environnement, qu'elles soient à visée offensive ou non. La décrédibilisation d'un chef militaire adverse, y compris par l'usage de fausses images ou rumeurs (*black psyops* selon le terme américain), désorganise ses propres forces mais également, dans une vision de la profondeur de l'action, lui aliène des soutiens. L'opération d'information, en tant que soutien de l'action offensive, se positionne ainsi naturellement au niveau des états-majors pour la conception et la conduite. Elle comporte aussi une composante de terrain chargée de l'exécution qui, selon les cas, peut être placée en arrière.

Toutefois il importe – c'est souvent la limite des actions d'information militaires – de prendre en compte une boucle de rétroaction subsidiaire. Avec la propagation incontrôlée – et surtout incontrôlable – des informations, au travers des réseaux sociaux en particulier, toute action militaire sur le terrain devient rapidement connue dans le monde entier, images à l'appui. L'expérience israélienne en 2006 le montre, la guerre de l'attention n'était pas tant au Liban que dans l'ensemble du monde. La facilité d'accès au cyberespace pour des mouvements non étatiques – ou même des États – démontre que l'action doit être permanente et en tous lieux. Les groupes non étatiques bénéficient d'ailleurs le plus souvent d'un avantage en termes de réactivité – et donc d'initiative – par leurs chaînes de commandement courtes, par rapport aux forces étatiques.

Figure 1. – Typologie des actions d'information



Daech, cas d'école de l'organisation infocentrée

L'irruption de Daech sur la scène internationale en 2013 a été aussi bien ressentie du point de vue de l'espace physique que dans le cyberespace. Daech n'a pas été le premier groupe armé terroriste à faire un usage

important du cyberespace et de l'information, loin s'en faut. Mais il a été le premier à professionnaliser et à industrialiser le processus, au point qu'il est possible de parler de l'organisation à son acmé (2014-2016) comme d'une machine de communication terroriste[8].

Les différents magazines, proposés en plusieurs langues (français, anglais, arabe, russe, etc.) visaient des publics spécifiques, surtout dans les pays occidentaux. Ces publications témoignent d'un haut niveau de professionnalisme avec l'utilisation probable de personnels formés avant leur départ ainsi que de journalistes capturés, et constituent l'un des éléments distinctifs de la propagande de l'État islamique. La séduction idéologique était également recherchée au travers de la forme, laquelle démontrait, d'une certaine manière, la puissance de Daech. Cette évolution du niveau qualitatif et graphique des publications de Daech permet aussi d'établir une chronologie de la puissance de l'organisation, le niveau des magazines augmentant avec l'extension géographique et la transformation en proto-État, pour ensuite décliner avec les pertes humaines et territoriales.

L'un des éléments les plus frappants dans la conflictualité informationnelle de Daech a été sa capacité à mobiliser des théologiens-rhéteurs de haut niveau chargés de contrer les messages émis par les autorités civiles, religieuses et militaires des camps opposés. Le décryptage des discours des ministres et chefs d'État occidentaux était au cœur des publications de l'organisation terroriste comme *Dar-Al-Islam* (en français) ou *Dabiq* (en anglais)[9]. Le démontage des opinions adverses, le contre-discours, la contre-propagande, que l'on pensait jusqu'ici être l'apanage des États et des organisations militaires, a été au cœur de la stratégie de communication de Daech. Il s'agissait ici pour l'État islamique d'apparaître comme une organisation étatique à l'identique des autres. Daech a démontré par son côté techno-réactionnaire la possibilité, pour une organisation infra-étatique, d'accéder à des outils de combat informationnel d'un niveau comparable à celui des pays les plus avancés.

La lutte pour l’attention comme enjeu majeur des guerres de demain

L’évolution prospective des technologies, en particulier liées au cyberespace (Internet des objets, intelligence artificielle, etc.), ouvre de nouveaux champs de possibilité en termes d’actions offensives utilisant l’information.

Un cyberespace plus ample et plus intrusif

Les changements en cours du cyberespace, en particulier sur le plan technologique, ouvrent de nouvelles possibilités de conflit en termes de combat informationnel. Le cyber est un domaine conflictuel artificiel qui transcende les espaces terrestre, maritime ou aérien. Il fournit un cadre d’action original puisqu’il est marqué à la fois par l’invariance stratégique de l’action sur les perceptions et par des spécificités uniques, comme, par exemple, la possibilité du camouflage de l’identité des acteurs et du lieu d’origine des attaques. Le cyber-conflit est par essence un conflit informationnel, y compris dans ses aspects techniques[10]. Les trois grands types de cyberattaques – sabotage, espionnage, subversion – sont des attaques infocentrées puisqu’il s’agit d’agir contre l’information (sabotage), pour l’information (espionnage) ou par l’information (subversion).

De fait l’augmentation exponentielle des informations produites dans le cyberespace donne aux acteurs malintentionnés un matériau de plus en plus important pour agir. En outre, les technologies cyber elles-mêmes, par leur sophistication technologique croissante, offrent des possibilités nouvelles de diffusion de l’information. Le *big data* qui procède à une analyse statistique ou semi-statistique des données informatiques en grand volume, permet, par corrélation des variables sociologiques, de créer des messages de plus en plus adaptés aux différentes catégories d’utilisateurs afin d’obtenir les

comportements recherchés, ce qu'a révélé le scandale autour de Cambridge Analytica lors de la campagne présidentielle américaine de 2016. L'Internet des objets recèle également des possibilités intéressantes, notamment la connexion au cyberespace de dispositifs de diffusion d'information. Des enceintes domestiques, des vêtements aux messages préprogrammés, des panneaux publicitaires interactifs, etc., peuvent être piratés pour en remplacer les contenus par des messages subversifs.

Des manipulations plus sophistiquées

L'intelligence artificielle (IA) offre quant à elle de nouvelles possibilités en termes défensifs, notamment *via* les techniques d'*user behaviour analysis* (UBA) qui cherchent par analyse du comportement de l'utilisateur à déterminer s'il y a une intrusion dans un système. Mais elle appartient aussi à une famille technologique dont les utilisations offensives sont patentes. Au-delà des emplois potentiels de l'IA dans l'informatique, il est également possible d'y voir des utilisations informationnelles. Le premier exemple notable est celui des faux particulièrement élaborés, appelés *deep fakes* en anglais, qui fleurissent depuis 2017 sur Internet.

Grâce à l'IA, il est maintenant possible de créer de fausses vidéos employant l'image et la voix de personnages connus (politiciens, hommes d'affaires, etc.) pour créer de faux discours. Ces nouvelles manipulations de l'information pourraient sans aucun doute être utilisées lors de conflits armés où la combinaison de l'image et de la voix de tel ou tel leader politique ou militaire servirait l'intérêt de ses adversaires[11]. Toutefois, plus que les outils techniques, il importe également de prendre en compte les canaux de diffusion.

La guerre de l'attention 3.0

Les réseaux sociaux qui sont apparus au milieu des années 2000 ont été la véritable révolution informationnelle portée par le cyberespace. Ils ont en effet aboli la frontière primordiale qui existait jusqu'ici entre producteurs et consommateurs d'informations. Avec les réseaux sociaux la communication est devenue un phénomène horizontal qui tend à remettre en cause chaque jour davantage le primat des journalistes et des médias traditionnels.

Dans le cadre des conflits armés, les réseaux sociaux ont été, plus encore que les cyberattaques « techniques », porteurs d'un pouvoir égalisateur. En effet, en l'absence de hiérarchisation des émetteurs d'information, le poids donné aux contenus émis par un État ou une force armée est, en théorie, comme en pratique, le même que celui accordé à un individu éclairé. Dans le domaine civil, une profession en ligne est ainsi née avec l'avènement de l'ère des réseaux, celle, protéiforme, d'influenceur. Dans le domaine militaire ou du moins conflictuel, les influenceurs sont rarement des individus assis sur une notoriété plus ou moins éphémère, mais sont le plus souvent des organisations qui promeuvent une vision et portent des messages au fort impact. Celles-ci qui sont des groupes combattants, des groupes armés terroristes ou non, rivalisent ainsi avec les forces gouvernementales « officielles », dans la bataille de l'attention ou, pour employer le terme anglo-saxon, du *narratif*. La guerre de l'attention 3.0 en ligne double la guerre physique conduite dans l'espace réel, les combats du terrain se superposant avec la guerre informationnelle entre protagonistes.

Un exemple frappant de cette guerre pour l'attention s'est déroulé en Afghanistan entre la force multinationale agissant sous commandement OTAN (ISAF) et les talibans, en particulier sur Twitter. Les deux organisations se sont affrontées par comptes Twitter interposés durant plusieurs années – les talibans recréant de nouveaux comptes à chaque clôture par Twitter, ce qui leur a malgré tout permis de disposer d'une quasi-permanence de communication – à l'occasion des diverses opérations

ou embuscades[12]. Il s'agissait ici de clamer sa victoire, de nier les capacités de l'adversaire ou d'exposer ses méfaits. En ce sens, l'espace informationnel des réseaux sociaux a dédoublé l'espace physique du combat avec une manipulation des perceptions d'une opinion publique potentiellement mondiale[13].

Les enjeux militaires afférents

La problématique actuelle pour les organismes militaires occidentaux – et avec eux les chercheurs spécialisés dans le domaine – est de faire face à une prétendue doctrine dite de la « guerre hybride » qui serait portée par la Russie dans le but de combiner les actions cinétiques traditionnelles d'un conflit avec des manœuvres informationnelles de désinformation et d'intoxication, en utilisant notamment en territoire ennemi des forces armées ne portant pas d'insignes d'identification. Cette « guerre hybride » se déroulerait ainsi à deux niveaux, à la fois tactique (sur le champ de bataille) et stratégique par la diffusion d'informations fausses ou biaisées.

S'affrontent ainsi deux visions stratégiques, celle d'un cyberespace avant tout technique où l'information a longtemps été une composante secondaire (espace euro-atlantique) et celle d'un cyberespace avant tout considéré comme espace informationnel (Russie et Chine). L'importance des doctrines stratégiques ou militaires liées à l'information rend compte de l'évolution de cette perception du champ informationnel comme zone d'intérêt majeure. La suprématie ou du moins la domination informationnelle est maintenant recherchée dans les conflits traditionnels.

L'explication de cette volonté de transformer progressivement le conflit en affaire centrée sur l'information se comprend en regard de deux composantes principales. Au sein des organisations militaires, les équipements et les combattants deviennent, par leur évolution technologique, des créateurs de données de plus en plus importants. Il en

découle, comme c'est le cas dans les forces armées françaises, une info-valorisation qui implique l'utilisation des données du terrain et du combat dans le but d'obtenir la suprématie sur le champ de bataille. Cette nécessité de l'info-valorisation est d'autant plus grande qu'elle est conçue pour dominer le champ de bataille [14].

Hors de celui-ci la composante de l'augmentation de la connectivité des populations au niveau mondial fait également du champ informationnel une zone de confrontation majeure pour les États et les armées. L'hyper-connectivité des populations, par ailleurs de plus en plus nomades, transforme les habitants des divers pays de la planète en spectateurs et en acteurs des conflits. Dès lors que l'on peut toucher en temps réel une majorité des habitants du monde, les actions informationnelles tendent à devenir des leviers majeurs pour agir sur les opinions publiques à une échelle industrielle par rapport aux précédents historiques.

*

Les opérations d'information dans le domaine militaire semblent appelées à se multiplier et à se complexifier. L'explosion de la communication qui va de pair avec une réduction exponentielle de la dimension espace-temps des médias, offre chaque jour davantage de poids à l'information prise au sens large. Alors que l'équation de la vérité face à l'immédiateté semble devoir être tranchée en faveur de cette dernière, les organisations militaires – étatiques ou non – devraient être en mesure de profiter de la situation. L'évolution prospective des technologies liées au cyberespace et aux médias, ainsi que l'intégration des leçons des conflits passés, pourrait créer un environnement informationnel toujours plus conflictuel.

Pour aller plus loin

GAT Azar, *A History of Military Thought : from the Enlightenment to the Cold War*, Oxford, Oxford University Press, 2001.

HÉMEZ Rémy, *Opérations de déception. Repenser la ruse au XXI^e siècle*, Paris, IFRI, 2018.

HUYGHE François-Bernard, KEMPF Olivier et MAZZUCCHI Nicolas, *Gagner les cyberconflits*, Paris, Economica, 2015.

US DOD, *Principles of Strategic Communication*, août 2008.

FOCUS 1

Le ciblage dans le domaine militaire

Lieutenant-colonel Éric Gomez

Le ciblage interarmées qui est particulièrement important dans le cadre de la planification militaire dépasse le champ de l'information ou du renseignement pour embrasser le domaine des opérations. Il est considéré comme un levier d'efficience pour l'action militaire et un outil primordial pour la maîtrise des risques en situation de combat. Il vise deux objectifs pendant une campagne militaire : porter atteinte de façon maîtrisée aux fonctions essentielles de l'adversaire ; amener cet adversaire dans la position militaire et politique que l'autorité politique de tutelle a définie comme permettant d'atteindre le but de guerre, ce que les militaires traduisent par l'état final recherché chez l'adversaire.

Le ciblage est un concept aussi ancien que la guerre, dont la pertinence a été rehaussée avec l'apparition de l'arme aérienne, puis du bombardement stratégique. En effet, les penseurs de l'aéronautique militaire ont rapidement cherché à aller au-delà des capacités limitées des aéronefs en matière d'emport en armements, tout en utilisant au mieux l'aptitude de la puissance aérienne à frapper l'ennemi dans la profondeur avec des munitions de plus en plus puissantes, agiles et précises.

En constante évolution au cours du XX^e siècle, le concept de ciblage interarmées ne se résume plus à présent à la seule action « cinétique », réalisée par tir d'artillerie, frappe aérienne, missile de croisière ou explosion au sol. Défini comme un « ciblage large spectre », il prend en compte non seulement la dimension létale, mais également la dimension non létale en coordonnant des actions réalisées dans les champs cinétiques, de l'influence militaire ou de l'action cybernétique. Le ciblage interarmées est un processus opérationnel s'appuyant sur le renseignement afin de bien connaître le système adverse, d'en identifier les faiblesses au regard de l'effet final recherché et de développer des cibles en anticipation afin d'être prêt à frapper dès les premières heures de la campagne militaire.

Toutefois, le terme « ciblage » s'avère difficile à appréhender dans le milieu militaire, car il est objectivé de façon différente par les spécialistes de la planification et de la conduite des opérations militaires, les membres des forces spéciales ou les spécialistes du renseignement, chacun lui attribuant un mode d'action et un but propre. Le point commun entre ces trois approches réside dans la nécessité d'un accès à une information abondante, pertinente et vérifiée afin de mener des actions précises et adaptées.

Le ciblage au XX^e siècle : de la frappe de masse à la « frappe chirurgicale »

Le ciblage est un besoin ancien des forces armées, mais il s'est peu à peu structuré autour de la composante aérienne, puis par la pratique des opérations. En effet, la recherche du point décisif permettant de l'emporter sur l'adversaire est inhérente à la stratégie militaire. Elle est développée par

de nombreux penseurs militaires, tels que Sun Tzu, Clausewitz, ou Jacques-Antoine-Hyppolite de Guibert, penseur militaire des Lumières.

Dans leur lignée, le général italien Giulio Douhet, premier théoricien des bombardements stratégiques, présenta cette vision stratégique appliquée aux opérations aériennes naissantes dans un traité intitulé *Il dominio dell'aria* (*La Maîtrise de l'air*) paru en 1921. Particulièrement marqué par les combats meurtriers de la Première Guerre mondiale, le général Douhet estimait que l'arme aérienne devait être l'outil privilégié pour briser les résistances morales et matérielles des belligérants. Il allait inspirer plusieurs militaires de haut rang au sein des armées britanniques et américaines.

Ainsi, au cours des années 1930, le général américain Billy Mitchell, actant le fait que la puissance aérienne était capable de survoler directement les centres vitaux de l'ennemi et de les neutraliser, théorisa le fait que l'arme aérienne pouvait mettre à bas très rapidement les capacités de résistance de la population adverse.

C'est notamment sur la base de ces théories que les aviations britanniques, puis anglo-américaines opérèrent, dès le début de la Deuxième Guerre mondiale, des campagnes intensives de bombardements stratégiques contre les infrastructures militaires et civiles du Troisième Reich. Compte tenu de la faiblesse des capacités de navigation des aéronefs de l'époque, les premières campagnes connurent un échec, démontré par le rapport Butt du 18 août 1941, selon lequel seul un avion sur trois parvenait à délivrer de l'armement à moins de huit kilomètres de son objectif.

S'inspirant en particulier des travaux réalisés par Solly Zukerman, médecin diplômé de zoologie que l'armée britannique employa pour participer au développement de la recherche opérationnelle, les aviations alliées s'attachèrent, avec le *Transportation Plan* de 1943, à frapper des cibles économiques, en particulier les centres ferroviaires, afin d'entraver les mouvements de l'ennemi et de fragiliser son potentiel industriel et économique. Dès lors les opérations aériennes alliées commençaient à

intégrer l’étude du système adverse et à peser sur ses centres de gravité et ses faiblesses afin d’amener l’ennemi à capituler.

Un apport théorique majeur apparut au cours de la première guerre du Golfe, avec la mise en application d’une théorie de bombardement stratégique, développée dans les années 1980 par le colonel John A. Warden III et connue sous le nom de théorie des 5 cercles. L’ennemi est analysé comme un système que l’on peut paralyser en frappant judicieusement les centres de gravité des différents cercles qui le constituent (commandement, éléments essentiels, infrastructures, population et forces armées). Cette stratégie se fonde sur la précision grandissante des armes que l’essor de l’armement guidé par laser ou par GPS a facilitée. Elle se fonde également sur l’usage de l’aviation comme arme principale. De plus, il ne s’agit plus tant de frapper la population civile que les infrastructures assurant la survie du système. Cela permet de limiter les dommages collatéraux tout en forçant l’ennemi à accepter une position.

Mise en application dans de nombreux conflits depuis 1991, la stratégie des 5 cercles de Warden s’avère cependant inopérante lorsqu’une armée régulière est confrontée à des mouvances non étatiques, organisées selon une tout autre logique. Elle trouve également ses limites dans un monde aux connexions moins rigides qu’autrefois. Pour répondre aux défis contemporains, la planification des actions militaires s’inscrit à présent dans la coordination d’actions létales et non létales, menées dans le cadre du ciblage large spectre.

Le ciblage large spectre : synchroniser les effets pour une efficacité accrue

Dans un contexte mondial ultraconnecté et face à l'émergence de la dimension cybernétique – quatrième dimension dans laquelle peut se porter le combat après la terre, l'eau et l'espace –, le ciblage interarmées ne peut plus être l'apanage du seul domaine cinétique, dont la préoccupation réside dans la délivrance d'une bombe, d'un obus ou d'un missile sur un objectif.

À ce titre, l'approche anglo-saxonne du *Full Spectrum Targeting*, ou « ciblage large spectre », prévaut au sein des états-majors stratégiques occidentaux depuis la crise libyenne de 2011. Il s'agit de faire converger les actions réalisées dans le domaine cinétique ou létal avec celles réalisées par des moyens non létaux, tels que l'influence militaire, les opérations de communication, la cyberguerre ou les actions de guerre électronique, entre autres. Le ciblage large spectre nécessite donc de combiner les actions réalisées simultanément ou de façon successive par une large variété d'effecteurs qui sont issus des forces spéciales comme des forces conventionnelles.

Ces effets sur le champ de bataille ou dans le champ des perceptions sont synchronisés, tout en étant généralement développés et suivis au niveau stratégique, c'est-à-dire par les plus hautes autorités politiques et militaires. Ils peuvent faire l'objet d'une coordination interministérielle, notamment entre les milieux militaires, diplomatiques et économiques, pour multiplier les leviers déployés contre l'adversaire et accroître l'efficacité des actions.

Ces actions nécessitent au préalable des analyses systémiques très complètes, réalisées en anticipation sur l'adversaire, afin de déterminer ses modes de fonctionnement, ses centres de gravité, ses forces et ses faiblesses au regard de la position politico-militaire vers laquelle l'action de la force doit l'amener. S'appuyant sur un renseignement abondant et précis, ces analyses sont des produits opérationnels permettant de réaliser ensuite des dossiers d'objectifs de différentes natures, en fonction des effecteurs qui seront chargés d'atteindre des effets sur l'adversaire.

Ainsi, ces dossiers d'objectifs peuvent être de nature cinétique, indiquant quels armements seront utilisés et de quelle manière, avec des préconisations relatives aux conditions d'emploi particulièrement fines. Mais ils peuvent également relever de l'influence militaire, dont le rôle consiste à mieux faire comprendre et accepter l'action de nos forces auprès des acteurs locaux et, ainsi, gagner leur confiance. Enfin, les dossiers d'objectifs peuvent relever du domaine cyber – un champ d'action nouveau qui émerge depuis une dizaine d'années.

Le cybernétique permet une gradation dans les actions. Il permet également d'atteindre une palette d'effets allant de la destruction à l'influence, comme l'illustre la propagande ciblée mise en œuvre en 2015 par des pirates pro-russes dans le Donbass, région frontalière de l'Ukraine avec la Russie. Les pirates s'étaient fait passer pour l'opérateur téléphonique local Kyivstar afin de diffuser de la propagande, de transmettre de fausses informations et d'inquiéter les militaires et gardes-frontières ukrainiens, ainsi que leurs familles, facilitant les actions menées par les forces paramilitaires pro-russes à leur encontre.

Le ciblage dans les opérations spéciales et les opérations de renseignement

Le ciblage est largement repris dans le cadre des opérations spéciales ou du renseignement. Il est alors perçu à travers un prisme particulier.

Dans le domaine du renseignement d'origine humaine, le ciblage désigne un ensemble d'opérations menées envers un individu ou une organisation afin d'envisager le recrutement d'une source. Une opération de ciblage permet alors de connaître l'environnement d'une source potentielle, les informations auxquelles elle pourrait avoir accès et les traits de sa

personnalité et de son histoire personnelle sur lesquels il faudra agir pour la recruter.

Dans le domaine des opérations spéciales, le ciblage est essentiellement vu comme un ensemble d'opérations visant à la neutralisation d'un objectif. Les processus engagés peuvent être les mêmes que ceux décrits dans le cadre du ciblage interarmées, mais l'effet à obtenir est généralement unique : la destruction de la cible.

La pratique du ciblage, qu'il concerne les opérations interarmées, les opérations de renseignement ou celles des opérations spéciales, soulève des questions éthiques et juridiques. En même temps, il permet de réduire les risques et d'assurer le respect de la loi des conflits armés.

Les opérations militaires sont contraintes par le droit international humanitaire (DIH), qui régit la conduite des conflits en définissant les cibles valides et la façon de procéder pour les atteindre. Ainsi, les populations adverses ne peuvent être frappées si elles ne sont pas identifiées comme étant combattantes ou comme aidant directement les forces combattantes. De même, de nombreux types de bâtiments ne doivent pas être détruits selon le DIH : les infrastructures essentielles pour la population civile, telles que les hôpitaux, mais aussi, par exemple, les lieux de culte.

Le ciblage interarmées permet de maîtriser les risques concernant les dommages collatéraux ou la destruction d'infrastructures non valides grâce à une analyse constante, à tous les niveaux du processus de développement de cible, relative à l'éligibilité des objectifs au regard de la loi internationale. Les objectifs sont également considérés en fonction du principe de proportionnalité entre l'importance militaire de la cible et le niveau de destruction décidé.

Pour aller plus loin

CLODFELTER Mark, *The Limits of Air Power : The American Bombing of North Vietnam*, Winnipeg, Bison Books, 2006, 312 p.

DOUHET Giulio (général), *La Guerre de l'air*, Paris, Éditions du journal *Les Ailes*, 1932, 190 p.

FOUCRIER Jean-Charles, *La Stratégie de la destruction. Les bombardements alliés en France en 1944*, Paris, Vendémiaire, 2017, 461 p.

SCHMITT Michael, DUCHEINE Paul, OSINGA Franz, *Targeting : The Challenges of Modern Warfare*, La Haye, TMC Asser Press, 2016, 299 p.

VAUTHIER P. (colonel), *La Doctrine de guerre du général Douhet*, Limoges, Lavauzelle, 1935, 274 p.

VILLIERS Pierre de (général d'armée), Allocution en conclusion du « Séminaire de la communauté militaire des opérations », Balard, 12 janvier 2016.

WARDEN John (colonel), *La Campagne aérienne*, Paris, Economica, 1998, 204 p.

CHAPITRE 2

Les couches basses du cyberespace : contrôle des flux et cartographie d'Internet

Kevin Limonier

Le 1er mai 2019, la Présidence russe promulguait la loi no 608767-7 sur la création d'un « Internet souverain ». Cette loi, qui est entrée en vigueur en novembre 2019, a pour objectif officiel de créer un système « alternatif » de transit des données pour échapper, notamment, au contrôle qu'exercent les États-Unis et leurs quatre alliés des *Five Eyes*[1] sur le réseau. Pour réaliser ce projet, l'ensemble de l'Internet russe est mis à contribution afin de réorganiser les infrastructures de câbles, de serveurs et de routage administrées depuis la Russie – constituant par là une rupture dans les modes de gestion et de gouvernance du Web. Sans même parler des conséquences politiques ou économiques qu'elle sous-tend, cette loi implique d'importants changements techniques sur ce que l'on appelle les « couches basses » du cyberespace, c'est-à-dire les systèmes dédiés à l'organisation des « tuyaux » physiques et virtuels d'Internet.

Jusqu'à présent, les routes d'Internet ne sont gérées par aucune autorité centralisée, à l'exception notable de quelques pays où Internet a été centralisé par l'État au début des années 2000, comme la Chine, l'Iran et la

Corée du Nord. La circulation des données sur le réseau, ainsi que leur acheminement, se fait sur la base d'un rapport de confiance réciproque entre les différents acteurs impliqués, au sein d'un réseau distribué[2]. Or, l'irruption de l'État russe comme entité régulatrice va à l'encontre de ce principe, soulevant des questions éthiques, politiques, économiques, mais également des problèmes de faisabilité technique. Avant d'inciter les acteurs de l'Internet russe à appliquer la loi en réorganisant le trafic des données, encore faut-il que les autorités aient une « vue d'ensemble » de l'architecture de leur réseau, et que celles-ci aient identifié les futurs points de contrôle stratégiques. Autrement dit, elles doivent d'abord connaître avec exactitude la structure (et la délimitation) des « couches basses » de segment du cyberespace pour faire appliquer la loi.

Dresser une cartographie suffisamment précise des différents protocoles de routage concernés par la nouvelle législation s'avère une tâche très complexe – voire une gageure méthodologique. Internet, et plus largement le cyberespace, constituent un ensemble de réseaux reliés les uns aux autres par une série de connexions physiques et de protocoles de routage ayant pour objectif d'acheminer des paquets de données numériques qui, une fois mis bout à bout, forment un message (texte, image, vidéo, etc.). Ce système, qui s'est développé de manière décentralisée et sans autorité de tutelle, est d'une complexité et d'une diversité difficilement concevables. Pour tenter d'y voir plus clair, cet enchevêtrement de connexions permettant à une information d'être à la fois envoyée, reçue, décodée et comprise (le tout en quelques millisecondes) est généralement pensé comme un système organisé en couches superposées et interdépendantes. Ce modèle en couches est structuré de manière verticale, les « couches basses » sont ainsi celles qui permettent aux « couches hautes » de fonctionner. Ce chapitre a pour objet de présenter le fonctionnement de ces couches basses et les enjeux géopolitiques sous-jacents à leur contrôle.

Les attributs de la couche infrastructurelle

Avant d'envoyer une information sur un réseau informatique, encore faut-il disposer des matériels nécessaires pour le faire, autrement dit d'un réseau physique. C'est l'objet de la première et de la plus basse des couches, dite « infrastructurelle ». Il s'agit concrètement des terminaux (smartphones, ordinateurs…) qui permettent d'avoir accès à l'information, mais aussi des infrastructures où les informations que l'on souhaite consulter sont physiquement inscrites (serveurs). Ce sont également les câbles transocéaniques, les dorsales de fibre optique, ainsi que les satellites permettant de faire transiter cette information entre le receveur et l'hébergeur de la donnée. Cette couche, qui est la plus basse de toutes, est aussi la plus facilement cartographiable puisqu'elle est constituée d'objets physiques localisables sur un planisphère à l'exception des objets spatiaux.

Cependant, il ne suffit pas de disposer d'un réseau physique pour pouvoir y faire circuler des données. Tout comme un réseau de chemin de fer a besoin d'aiguillages pour éviter l'engorgement des lignes ferroviaires, Internet s'organise autour de protocoles de routage et d'adressage qui permettent aux paquets de données d'atteindre leur destination sans se perdre et en minimisant les risques de congestion. Ces systèmes de routage constituent la deuxième couche, dite des « protocoles », dans la mesure où la circulation des données est normée par toute une série de protocoles tels que le TCP/IP, le Border Gateway Protocol (BGP), qui permet aux sous-réseaux d'Internet de communiquer entre eux, ou encore le protocole DNS (Domain Name System), qui permet de faire correspondre des adresses IP avec des noms de domaine et qui constitue la base du système des hyperliens que nous utilisons quotidiennement.

La couche physique et la couche des protocoles forment ainsi les « couches basses » qui organisent la circulation des données, par opposition aux « couches hautes » qui organisent quant à elles la circulation de

l’information (c’est-à-dire des données décodées et décodées par des plateformes d’intermédiation). Les tentatives de régulation ou de contrôle d’Internet par l’État sont généralement observées et commentées à partir de ce qui se passe dans les couches hautes, sans doute parce que les mécanismes de pouvoir et les enjeux politiques y sont plus immédiatement visibles. Ainsi est apparue la problématique de la gouvernance du cyberespace, tandis que les plateformes d’intermédiation sont devenues des acteurs à part entière dans bien des rapports de force.

Les enjeux du contrôle des couches basses

Peu étudiées en comparaison[3], les couches basses n’en sont pas moins des objets de plus en plus centraux de la géopolitique, au sens où la définit Yves Lacoste, c’est-à-dire comme des éléments stratégiques, en cela qu’ils peuvent être mobilisés par des acteurs pour s’assurer ou contester le contrôle d’un territoire[4].

Si ces objets sont stratégiques, il en va de même des savoirs qui permettent de les identifier et d’en comprendre le fonctionnement. Cependant, à l’exception de la localisation des infrastructures, l’organisation des couches basses du cyberespace relève de savoirs techniques généralement peu accessibles au géographe et, plus largement, au chercheur en sciences sociales s’intéressant aux processus de domination et de contrôle. Pourtant, depuis que les protocoles IP, BGP, DNS (pour ne citer qu’eux) permettent chaque jour de transporter des volumes de données toujours plus importants, ils s’imposent à nous comme des éléments incontournables à la fois de nos vies quotidiennes et des rapports de force internationaux.

La législation russe de 2019 sur un « Internet souverain » constitue un tournant en cela qu’elle présuppose une cartographie des interactions au

niveau physique et protocolaire. Ce double objectif montre combien l'analyse des mécanismes de routage des données est devenue un « savoir stratégique » nécessaire à l'élaboration d'un contrôle territorial. Par ailleurs, l'analyse de ces protocoles permet d'en finir avec l'idée qu'Internet marquerait la « fin de la géographie[5] », l'immédiateté de la transmission des informations annulant la contrainte espace-temps et abolissant les frontières politiques. Au contraire, les routages, en tant qu'interconnexions virtuelles entre divers éléments du réseau, remettent la spatialisation au centre du raisonnement. La connaissance du réseau à des fins de contrôle (ou de contournement du contrôle) présuppose en effet d'en élaborer des cartes qui, souvent, devront s'affranchir de la topographie pour prendre la forme de graphes. Autrement dit, l'étude des stratégies de contrôle du réseau postule le développement de méthodologies de représentation graphique et d'analyse qui s'inspirent aussi bien de l'analyse géopolitique des réseaux[6] que de la théorie des graphes[7] et de celle de l'acteur-réseau[8].

Les « briques élémentaires » d'Internet

Internet est, comme son nom l'indique, un réseau de réseaux (*inter-network*). Véritables « briques élémentaires » d'Internet, les sous-réseaux qui le composent sont appelés systèmes autonomes (*autonomous systems*, ou AS). Typiquement, un AS peut être un fournisseur d'accès Internet, le réseau d'une grande université, d'un ministère, ou encore un gestionnaire de dorsales de fibre optique. Ils sont dits « autonomes » dans la mesure où chaque AS répond à ses propres politiques de routage.

Véritables politiques d'aiguillages des données sur le réseau, les routages répondent à un certain nombre de protocoles standardisés. Ceux-ci permettent à tous ces systèmes autonomes de « se comprendre » et de parler la même langue. Ainsi, l'IP (Internet Protocol) organise les routages sur la

base d’adresses numériques allouées à chaque machine connectée. Le protocole DNS (Domain Name System) permettra quant à lui de faire correspondre adresses IP et noms de domaine.

Tous ces protocoles ne sauraient fonctionner s’il n’en existait pas un dont le rôle est d’assurer le transit des données entre les différents systèmes autonomes qui composent Internet. C’est le rôle du BGP, le Border Gateway Protocol. Relativement méconnu par rapport à l’IP ou au DNS, le BGP a un rôle central dans le fonctionnement d’Internet, c’est en effet lui qui relie entre eux les milliers de systèmes autonomes dont Internet est composé[9]. Concrètement, pour que deux systèmes autonomes puissent échanger des données, il faut qu’ils aient contracté un « accord BGP » (*BGP agreement*) – c’est-à-dire une entente, contractuelle ou non, qui régit les modalités selon lesquelles deux systèmes autonomes vont échanger des données.

Or, aucun AS n’entretient d’accord BGP avec la totalité des autres AS qui constituent Internet, dans la mesure où ces relations sont le produit de relations contractuelles entre les gestionnaires de réseaux, et sont donc le fruit de négociations commerciales, voire politiques. Autrement dit, les accords entre systèmes autonomes sont le fait d’opérateurs humains, même s’ils sont ensuite gérés au quotidien par des systèmes automatiques (routeurs) qui ont la tâche de choisir le chemin le plus court pour acheminer un paquet de données d’un point A à un point B d’Internet. La principale conséquence de ce constat est que, pour parvenir d’un point A à un point B, un paquet de données passera généralement par des AS intermédiaires, en suivant la structure BGP du réseau Internet.

Figure 2. – Schéma du fonctionnement d'Internet

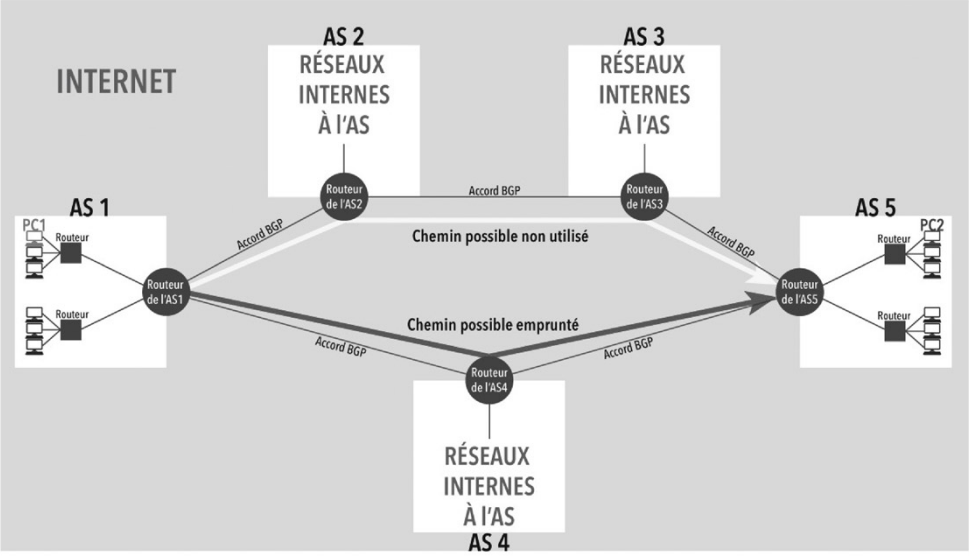


Schéma élaboré par Louis Pétiniaud

Le voyage d'un paquet de données

Les AS sont avant tout composés d'infrastructures physiques. Ainsi, pour parvenir d'un point A à un point B du réseau, notre paquet devra voyager entre routeurs et câbles – c'est-à-dire *via* des infrastructures physiques localisables à la surface du globe.

À titre d'illustration, prenons ici l'exemple d'un paquet de données envoyé depuis New York vers Moscou. Ce paquet suivra un chemin déterminé par des accords BGP, en passant d'un AS à l'autre jusqu'à arriver à celui de son destinataire.

On peut suivre en temps réel un tel « voyage » en utilisant la commande Traceroute, disponible sur la plupart des systèmes d'exploitation grand public. À l'origine développée pour les gestionnaires de réseaux complexes, cette commande nous permet de visualiser le « voyage » d'un paquet de données au sein d'un réseau informatique, à chaque fois que le paquet

traversera un routeur, il renverra à son expéditeur un signal l'informant qu'il l'a bel et bien traversé.

Tableau 1 – Une commande Traceroute

1	router2-nac.linode.com.	**Linode, LLC** AS8001	1.0 ms
2	—	**Linode, LLC** AS63949	0.7 ms
3	et-0-0-29.cr3-nyc3.ip4.gtt.net.	**GTT Communications Inc.** AS3257	2.0 ms
4	xe-0-1-0.cr1-stk3.ip4.gtt.net.	**GTT Communications Inc.** AS3257	104.3 ms
5	rostel-gw.ip4.gtt.net.	**GTT Communications Inc.** AS3257	123.9 ms
6	—	**Rostelecom** AS12389	129.2 ms

Le tableau ci-dessus reproduit une commande Traceroute effectuée le 22 octobre 2019 depuis un serveur situé à New York. Ce serveur a envoyé un paquet de données vers Moscou, et plus particulièrement vers l'AS de Rostelecom, l'opérateur historique russe. Traceroute permet de visualiser les routeurs précis par lesquels notre paquet de données est passé avant d'arriver à destination. On constate ici qu'il a fallu six « sauts » (*hops*) à ce paquet pour voyager de New York à Moscou, et qu'il est passé par 4 AS différents : les AS8001 et AS63949 (qui appartiennent à un FAI appelé Linode), l'AS32527 (propriété de GTT Communications, une entreprise allemande administrant plusieurs câbles sous-marins) et enfin l'AS12389, propriété de Rostelecom. Autrement dit, notre paquet de données est passé par au moins six routeurs différents, répartis en divers points du globe.

Dès lors, il est théoriquement possible de tracer sur un planisphère la route qu'a empruntée notre paquet de données. On insistera sur le « théoriquement », dans la mesure où plusieurs difficultés techniques, telles que le géocodage des adresses IP[10], limitent la précision avec laquelle on peut espérer localiser un routeur. Pour autant, diverses informations dévoilées par notre commande Traceroute permettent de déduire le chemin

précis emprunté par notre paquet de données, avec une certaine marge d'incertitude.

Concrètement, un accord BGP se matérialise par une connexion physique entre les routeurs de deux AS. Or, ces branchements sont généralement mis en œuvre dans des infrastructures dédiées à cet effet : les Internet eXchange Points (IXP), où les routeurs de divers AS sont reliés les uns aux autres. Il existe aujourd'hui plusieurs centaines d'IXP dans le monde, et ces infrastructures constituent des points hautement stratégiques d'Internet : si un ou plusieurs IXP d'envergure mondiale venaient à être mis hors d'état de fonctionner, cela aurait probablement pour conséquence d'isoler certains systèmes autonomes. Pour un utilisateur, cela signifierait qu'il ne pourrait plus communiquer avec des personnes connectées *via* un autre fournisseur d'accès ou opérateur mobile que lui.

Outre les connexions à l'intérieur des IXP, il faut également prendre en compte celles qui relient ces infrastructures entre elles. Les IXP sont reliés entre eux par tout un réseau de câbles terrestres et sous-marins par lesquels passent entre 90 % et 99 % des données échangées quotidiennement par l'humanité (les 1 % à 10 % restants sont transportés par satellite[11]), et qui constituent « l'épine dorsale » (*backbone*) d'Internet : qu'un câble majeur vienne à être coupé, et le trafic sera fortement perturbé, voire, s'il n'existe pas de route alternative, totalement interrompu.

Dans notre exemple, et partant des informations rendues disponibles par les IXP, les AS et les administrateurs de câbles, on peut déduire du chemin emprunté par notre paquet de données qu'il a traversé son premier routeur dans un IXP situé à Buffalo, sur les rives du lac Érié (État de New York). C'est là que le réseau Linode l'a « confié » à GTT Communications. De là, notre donnée a été acheminée en Europe, probablement *via* le réseau canadien de GTT, qui relie les Grands Lacs à l'Atlantique en suivant l'axe de communication que représente le fleuve Saint-Laurent. Ensuite, notre donnée a plongé dans l'océan au niveau d'Halifax (Nouvelle-Écosse) pour

ressortir à Dublin *via* le câble sous-marin GTT Atlantic, qui suit d'ailleurs le tracé des vieux câbles télégraphiques de la fin du XIX^e^ siècle. Notre paquet a ensuite été transmis à Rostelecom, probablement *via* le DE-CIX Frankfurt, le deuxième plus important IXP du monde et véritable *hub* européen de données. De là, il a été convoyé par Rostelecom *via* le câble terrestre Fastline, qui relie Francfort à Smolensk, puis Moscou, destination finale de notre paquet.

Déni d'accès, espionnage et contrôle de l'information

Ici, notre paquet de 60 bytes a voyagé sans encombre. Pourtant, de nombreuses embûches auraient pu se dresser sur son chemin. Que ce soit à des fins de contrôle, de censure, de déni d'accès ou même de destruction pure et simple, différentes techniques de manipulation des routages existent, qui sont désormais utilisées par des acteurs étatiques ou non étatiques dans le cadre de stratégies de contrôle territorial.

Nous l'avons vu, les routes d'Internet sont à la fois topologiques et topographiques : elles sont composées des chemins en eux-mêmes (câbles), sur lesquels interviennent des aiguilleurs (routeurs) selon des politiques de gestion des flux (BGP). De la même manière, on peut distinguer les stratégies géopolitiques visant le réseau physique (topographie) de celles visant le réseau virtuel et les mécanismes de routage (topologie).

Les manipulations physiques du réseau

Sur le réseau physique, les actes visant à perturber le trafic à des fins géopolitiques consistent en des manœuvres classiques de sabotage et de

destruction d’infrastructures. Le premier exemple qui vient à l’esprit est naturellement celui des câbles, qui peuvent être coupés. Plusieurs fois déjà, des opérations militaires ont été accompagnées de destructions de dorsales afin de limiter les moyens de communication de l’ennemi. Ce fut le cas en Géorgie en 2008, lorsque les câbles reliant Sotchi au port géorgien de Poti furent débranchés. En Crimée également, les câbles reliant la péninsule à l’Ukraine continentale *via* l’isthme de Perekop furent mis hors d’état de fonctionner par les forces russes ayant investi la région en 2014.

D’une manière générale, la rupture de dorsale est un événement très perturbateur pour la cohésion du réseau de l’État visé. En effet, qu’un câble vienne à être coupé et les données l’empruntant d’ordinaire seront reroutées vers un chemin alternatif avec comme conséquence une baisse drastique de la bande passante. Parfois, le territoire en question peut être totalement coupé du monde, lorsqu’il n’existe pas de chemin alternatif possible. C’est ce qui s’est passé aux îles Tonga au début de l’année 2019, lorsque ce petit archipel du Pacifique fut coupé du reste du monde après la rupture d’un câble sous-marin.

La question de la résilience devient alors cruciale pour de nombreux pays qui dépendent d’un ou de deux câbles. Ainsi, la Géorgie s’est depuis 2008 dotée d’un câble traversant la mer Noire jusqu’en Bulgarie afin d’éviter la Russie. Ce câble, par lequel transite l’écrasante majorité du trafic Internet géorgien, a d’ailleurs un temps été convoité par un opérateur russe – avant qu’une campagne médiatique ne vienne arrêter cette tentative de rachat alors qualifiée « d’abandon de souveraineté ».

Les manipulations de routage

D’une manière générale, la perturbation des routes d’Internet par destruction physique d’infrastructures demeure rare. Si l’on omet les stratégies de prise de contrôle économique, ce sont des actes qui se situent

dans le spectre de la guerre conventionnelle et qui, de ce fait, ne souffrent souvent d'aucune équivoque quant à l'intention de l'attaquant – au contraire des manipulations de routage.

En effet, autant une destruction d'infrastructures s'avère être un phénomène classique de coercition, autant la manipulation des routes d'Internet au niveau des protocoles permet de s'affranchir de tout dommage physique – voire même de toute possibilité d'identification de l'attaquant. Rappelons que les interconnexions BGP sont fondées sur un rapport de confiance entre les systèmes qui s'échangent en permanence nos données. En d'autres termes, les routeurs ne sont pas censés se mentir les uns aux autres.

On peut alors aisément imaginer que l'immixtion d'un acteur mal intentionné dans ce système fondé sur la confiance puisse avoir des conséquences dramatiques. Il sera en effet possible à celui-ci d'usurper l'identité d'un système autonome légitime afin de rerouter vers lui un trafic qui ne lui était pas destiné.

Ce type d'attaque dite de « l'homme du milieu » (*middle man attack*) permet ainsi, en toute discrétion, de détourner, d'espionner un flux de données ou même d'injecter, dans des paquets sains, des éléments malveillants. Ainsi, en 2013, plusieurs chercheurs de Renesys avaient remarqué que plusieurs flux de données nord-américains s'étaient subitement mis à passer par la Biélorussie – sans que l'on sache exactement s'il s'agissait d'un acte malveillant ou d'une erreur technique[12].

En effet, une manipulation des routages BGP peut aussi bien être le fruit d'une erreur humaine, comme cela arrive des dizaines de fois par jour. Parfois, ces erreurs sont si spectaculaires qu'elles éveillent nécessairement les soupçons – comme lorsqu'en juin 2019, une part significative du trafic du FAI français Bouygues Telecom fut subitement reroutée vers la Chine[13]. Dû à une erreur commise par un technicien dans un *datacenter* en Suisse,

cet événement a souligné combien les routes d'Internet sont fragiles et peuvent être manipulées à grande échelle.

Si elle s'avère un intéressant outil d'espionnage et de coercition externe, la manipulation des routes d'Internet constitue également un puissant levier de contrôle des populations. Certes, à ce jour, rares sont les pays à avoir mis en place un véritable système de contrôle de leur trafic au niveau BGP – la plupart des pays se contentant d'un blocage DNS facilement contournable à l'aide d'un VPN. Pour autant, on peut citer l'exemple de la Chine et de l'Iran, où le réseau Internet s'est construit de façon à limiter au maximum les points d'entrée et de sortie du réseau national. Ainsi, le réseau iranien ne compte que trois ou quatre AS directement connectés à des systèmes étrangers, si bien que la totalité du trafic entrant et sortant du pays doit traverser leurs routeurs. C'est notamment cette architecture très particulière qui a permis aux autorités de bloquer Internet dans le pays en novembre 2019.

Si la Chine et l'Iran ont la possibilité de contrôler leur réseau de manière aussi efficace, c'est que la structure du routage a été pensée dans cette perspective au moment où Internet s'est développé – ce qui n'est pas le cas dans la plupart des pays du monde. Ainsi, la Russie est confrontée à d'importantes difficultés dans la mise en place des conditions techniques lui permettant d'appliquer sa loi sur un « Internet souverain ». Là où les réseaux iranien et chinois se sont construits selon un plan centralisé et sous l'égide des autorités, celui de la Russie est le résultat de vingt années de développement libre – et parfois chaotique – d'un réseau qui compte parmi les plus complexes du monde. Concrètement, cela signifie qu'il existe de très nombreux AS et, *in fine*, de très nombreuses routes permettant d'entrer et de sortir du territoire russe. Dès lors, la Russie est engagée dans un processus de centralisation et de rationalisation de son réseau – indispensable à l'application de sa nouvelle législation. Or, la tâche s'annonce complexe : le pays compte plusieurs milliers de fournisseurs

d’accès (là où la France en compte moins d’une dizaine) et, parmi eux, un certain nombre refusent de se plier aux injonctions du pouvoir, quitte à risquer de longues procédures judiciaires[14]. Certains n’hésitent d’ailleurs pas à publier les injonctions qu’ils reçoivent du FSB[15].

*

Cartographier les routes d’Internet pour y appliquer un raisonnement géopolitique s’avère un exercice complexe. Les nombreuses incertitudes que recèle la collecte des informations nécessaires pour comprendre comment un paquet de données « voyage » d’un point à l’autre du cyberespace doivent être croisées avec des informations géographiques souvent parcellaires. Le « savoir stratégique » induit par cette cartographie est donc lui-même flou – rendant l’action des acteurs incertaine lorsque l’on dépasse une certaine échelle de complexité. Pourtant, et malgré cette connaissance parcellaire, un nombre croissant d’acteurs n’hésitent plus à « manipuler » les routes d’Internet à des fins de contrôle ou de puissance – sans forcément avoir la capacité d’apprécier l’ensemble des conséquences de leurs actions. C’est bien là le paradoxe d’opérations menées sans cartes précises du champ de bataille.

Pour aller plus loin

ALLEN John, *Topologies of Power : Beyond territory and networks*, Londres, Routledge, 2016.

BARAN Paul, *On Distributed Communications : I. Introduction to Distributed Communications Networks*, Santa Monica, RAND Corporation, 1964.

ERMOSHINA Ksenia et MUSIANI Francesca, « Migrating servers, elusive users : Reconfigurations of the Russian Internet in the post-Snowden era », *Media and Communication*, 22 mars 2017, vol. 5, n° 1, p. 42.

LACOSTE Yves, *La géographie, ça sert, d'abord, à faire la guerre*, Paris, La Découverte, « La Découverte Poche/Essais », 2014, édition augmentée, 249 p.

LAW John, *A Sociology of Monsters : Essays on Power, Technology and Domination*, Londres, Routledge, 1991.

LE BÉCHEC Mariannig, « Le territoire comme un graphe. Pratiques, formes, éthique », *Les Cahiers du numérique*, 2016, vol. 12, n° 4, p. 131-156.

MUIR James A. et OORSCHOT Paul C. (van), « Internet geolocation : Evasion and counterevasion », *ACM Comput. Surv.*, décembre 2009, vol. 42, n° 1, p. 4 : 1-4 : 23.

STAROSIELSKI Nicole, *The Undersea Network*, Durham, Duke University Press, 2015, 292 p.

VIRILIO Paul, « Fin de l'histoire ou fin de la géographie ? Un monde surexposé », *Le Monde diplomatique*, août 1997.

FOCUS 2

La guerre électronique

Lieutenant-colonel Éric Gomez

La guerre électronique est un espace de conflictualité apparu au début du XX^e^ siècle avec les premiers moyens de télécommunication. Instaurée par des acteurs économiques à la recherche de moyens de communication, elle est devenue l'apanage de l'affrontement militaire avant d'en dépasser largement le cadre. Elle a évolué au rythme des technologies de l'information, s'adaptant à l'émergence de la télégraphie, puis de la radio, de la technologie radar, des communications satellitaires ou mobiles et de l'Internet. Son usage a aussi été façonné par de nombreuses crises géopolitiques et de multiples conflits.

La guerre électronique consiste à exploiter le spectre électromagnétique dans le but de combattre un adversaire ou de s'en protéger. Le spectre électromagnétique désigne la répartition des ondes électromagnétiques en fonction de leur longueur d'onde, de leur fréquence ou de leur énergie. Dans le cadre militaire, il est utilisé pour générer une asymétrie de l'information en réduisant la part d'incertitude dans son propre camp et en désorganisant l'ennemi. Il s'agit d'être capable de mieux comprendre l'environnement de combat, de conserver liberté d'action et fulgurance

grâce à la transmission de l'information, tout en gênant l'adversaire dans sa manœuvre. Dans certaines configurations, la guerre électronique peut désorganiser l'adversaire et, ainsi, contribuer directement à sa défaite.

Les débuts de la guerre électronique

À la fin du XIX^e^ siècle, à la suite de la création du télégraphe électrique en 1844, du téléphone de Bell en 1876, puis de la télégraphie sans fil (TSF) de Marconi en 1896, les milieux économiques intégrèrent très rapidement ces technologies de l'information dans leurs modes de fonctionnement. Ils comprirent également l'intérêt d'écouter leurs concurrents et de les brouiller. C'est ainsi que des agences de presse, s'adonnant à une concurrence rude et déloyale, donnèrent naissance dans les années 1890 à la guerre électronique. Celle-ci intégra le domaine militaire lors du conflit russo-japonais de 1904-1905, au cours duquel la mise en œuvre d'opérations d'écoutes et de brouillage a permis aux Japonais de suivre la progression de la marine impériale russe.

La Première Guerre mondiale donna lieu à la première exploitation militaire importante du spectre électromagnétique avec l'utilisation de réseaux radio militaires, l'écoute et la localisation de ces émissions. La guerre électronique prit alors une importance de premier ordre pour les états-majors et les opérations, permettant d'obtenir du renseignement de niveau stratégique et tactique.

Dans les années 1930 apparurent la radiogoniométrie[1] à usage civil pour la navigation aérienne et maritime, puis la technologie radar. Dans ce nouveau contexte technologique, l'amiral Raoul Castex théorisa une « guerre des communications » dans le milieu maritime, associant « corsaires sous-marins et de surface », escadres et avions basés à terre, tous

connectés par radio et capables de générer un effet de saturation sur l'adversaire.

Cette vision stratégique devait se confirmer lors de la Seconde Guerre mondiale, la guerre électronique jouant un rôle majeur dans la conduite de la guerre et l'emploi d'armements modernes. Ainsi, les actions de leurrage des radars de la défense aérienne adverse lors des raids de bombardiers, l'usage de la radiogoniométrie dans la lutte contre les U-Boot allemands dans l'Atlantique ou les actions de déception réalisées en soutien de l'opération *Overlord* en Normandie le 6 juin 1944 furent déterminantes dans les opérations engagées par les alliés.

Des ondes radio au cyberespace

L'apparition des capacités de frappes nucléaires et la mise en place du rideau de fer créèrent la nécessité d'un accès au-dessus des territoires visés et d'un renseignement performant. L'utilisation du spectre électromagnétique fut donc renforcée pendant la guerre froide dans le cadre de l'espionnage, mais aussi du développement d'armements permettant de prendre l'avantage en cas de confrontation directe.

De nombreuses stations d'écoutes furent ainsi installées par les protagonistes en des lieux jugés stratégiques, tels que l'Allemagne ou le Canada, tandis que des plateformes aéronautiques et maritimes furent équipées de systèmes d'écoutes, de localisation ou de brouillage. De nouvelles technologies furent également développées dans ce sens, comme l'illustrent l'utilisation de la réflexion électromagnétique sur la Lune pour détecter les radars soviétiques, les vols d'avions U2 au-dessus du territoire soviétique dans les années 1950 ou le développement de satellites de communication et d'écoutes électromagnétiques à partir des années 1960.

Le spectre électromagnétique permit également d'améliorer certains armements pour porter atteinte aux capacités de défense de l'adversaire. On peut citer les victoires aériennes américaines grâce à l'utilisation de missiles guidés par infrarouge *Sidewinder* en 1958 durant la deuxième crise du détroit de Taïwan ; la destruction d'un avion de reconnaissance U2 américain en 1960 par un missile sol-air soviétique ; l'utilisation déterminante de la guerre électronique durant la crise de Cuba, puis pendant la guerre du Vietnam avec, notamment, les missions d'avions F105F *Wild Weasel II* qui permettaient de neutraliser les batteries SA2 détenues par le Nord-Vietnam.

Des avancées technologiques dans le champ électromagnétique ont en outre permis d'améliorer la force de frappe des armements contemporains : les premières frappes aériennes utilisant des missiles guidés par laser ont lieu pendant la guerre du Vietnam ; l'introduction de peintures atténuant les réflexions électromagnétiques et l'adoption de formes limitant la surface équivalente radar (SER) ont conduit à un emploi intensif des avions furtifs F-117 lors de la guerre du Golfe, puis durant la guerre du Kosovo.

Ces techniques de contre-mesure électronique restent à l'œuvre pour les armements modernes, tels que les chasseurs de quatrième génération (le Rafale français) ou de cinquième génération (le F35 américain) ou les navires furtifs (par exemple les navires de classe Horizon en France). De manière générale, la guerre électronique est une préoccupation constante lors de la conception de nouveaux équipements, intégrant toujours plus avant le domaine numérique.

La guerre électronique à l'ère numérique

Le volet le plus moderne de la guerre électronique est lié à l'omniprésence des réseaux informatiques à partir des années 1970. Créé en

1973, le réseau militaire américain Arpanet, ancêtre d'Internet, devait être séparé dix ans plus tard en deux réseaux distincts, Milnet pour les militaires et Arpanet/Internet pour les universitaires, avant que ce dernier réseau ne devienne, en 1995, une interconnexion de réseaux privés.

La révolution de l'information induite par ces technologies a mené à la création d'un nouveau champ de confrontation, éthéré et dématérialisé, mais extrêmement puissant : celui de la dimension « cyber ». Initialement inclus au sein de la guerre électronique, le cyber s'en est affranchi progressivement tout en la complétant, comme l'illustre notamment le conflit de 2014 en Ukraine, au cours duquel les forces russes ont réussi, par des actions de piratage informatique, à déstabiliser les réseaux de communication ukrainiens et à localiser des objectifs militaires pour réaliser des frappes de précision.

Nouvel espace de conflictualité, le cyber se prête parfaitement à des actions de guerre électronique déclinées du niveau stratégique au niveau tactique. En effet, il reste tributaire du signal qui le diffuse et constitue le cœur de cible de la guerre électronique : pour mener une action cyber, il faut avoir accès au spectre électromagnétique et le maîtriser. Enfin, deux avancées technologiques et doctrinales majeures de ce début de XXI^{e} siècle laissent entrevoir un rebond dans les actions de guerre électronique : la numérisation du champ de bataille terrestre et le « combat multidomaines ».

La numérisation du champ de bataille est largement mise en œuvre depuis près d'un demi-siècle pour les dimensions aéronautique et maritime, comme l'illustre, par exemple, l'utilisation d'avions AWACS pour coordonner les actions simultanées de nombreux avions. Toutefois, au niveau du combat terrestre, elle ne l'était pas jusqu'à l'arrivée de nouveaux équipements au sein des armées de terre occidentales permettant de connaître en temps réel la position des troupes amies et la situation tactique. La gestion du champ de bataille terrestre est ainsi rapidement passée de la numérisation à l'info-valorisation, rehaussant nettement le niveau

d’appréciation de la situation générale par les commandeurs terrestre et interarmées.

Dans ce contexte, la conduite des opérations interarmées et interdomaines (terre, air, mer, cyber, espace) tend vers une meilleure intégration des manœuvres dès le niveau tactique afin de tirer parti en temps réel des opportunités et de limiter les difficultés générées par les dépendances intermilieux[2]. Appelé « combat multidomaines », ce mode de fonctionnement nécessite une organisation de la conduite des opérations (C2 en langage militaire) évolutive et agile, capable de distribuer de façon dynamique les fonctions et les responsabilités au plus près de l’action, afin d’assurer la continuité des opérations.

Cette évolution permet d’envisager une meilleure intégration de la manœuvre interarmées, qui bute souvent sur des logiques de milieu ou de cultures d’armées. Face au « combat multidomaines », la guerre électronique joue un rôle fondamental pour gêner la conduite des opérations et empêcher les armées modernes d’utiliser de la meilleure façon cette numérisation des espaces de confrontation. En contestant à l’adversaire l’accès au spectre électromagnétique, les armées modernes bénéficieront d’un avantage informationnel et créeront une véritable asymétrie dans les conditions de conduite de la guerre.

*

Depuis le début du XX^{e} siècle, l’information s’est progressivement confondue avec l’informatique et l’électronique. Poursuivant une mutation engagée dans ce contexte, la guerre électronique a totalement intégré le domaine de la guerre de l’information depuis que le spectre électromagnétique est devenu essentiel au transport de l’information.

Grâce notamment aux écoutes ou au brouillage, la guerre électronique porte la conflictualité dans la sphère de l’information. À cet égard, le domaine cyber, initialement inclus dans la guerre électronique, en prolonge

les actions. Il reste cependant étroitement dépendant de la guerre électronique, dès lors que le spectre électromagnétique sert de support au déploiement des outils cybernétiques.

À l'orée du XXIe siècle, la prise en compte des nouvelles technologies dans l'évolution de la conduite des opérations, permet aux armées modernes de conserver une réactivité et une cohérence d'action supérieures à celles de leurs adversaires, et confère à la guerre électronique une position privilégiée pour réduire, voire neutraliser, les capacités adverses.

Pour aller plus loin

LETERTRE Olivier, JUSTEL Patrick, LECHÂBLE Romain et DOSSÉ Stéphane, « Regards croisés sur la guerre électronique », *Focus stratégique*, IFRI, juillet 2019, no 90.

SIFFRE Jean-Paul, *La Guerre électronique. Maître des ondes, maître du monde*, Limoges, Lavauzelle, 2003.

TERRIEN Olivier, *Les 36 Stratagèmes de la guerre électronique*, Mérignac, Oty Productions SAS, janvier 2012.

CHAPITRE 3

Les techniques d'amplification sur les réseaux sociaux[1]

Ben Nimmo

C'est la grande force des réseaux sociaux que d'offrir une voix à ceux qui n'en ont pas. Les médias traditionnels rapportent souvent ces histoires d'utilisateurs, jusqu'alors inconnus, qui font « le buzz » sur les réseaux sociaux et deviennent célèbres en publiant un message simple dont le contenu peut être positif[2], négatif[3] ou, très simplement, exprimer une envie de croquettes de poulet[4].

Ce pouvoir en question offre aux opérations informationnelles la possibilité d'étendre leur portée bien au-delà de ce qui aurait été possible quand les médias traditionnels étaient la seule véritable option. En effet, ces utilisateurs « sans voix » ne sont pas toujours des individus en chair et en os : ils peuvent être des comptes coordonnés, détournés, loués, ou tout simplement créés dans le seul but d'amplifier un message sur les réseaux sociaux.

Pour paraphraser Shakespeare, nous pouvons dire que quelques messages sont nés pour la grandeur, par exemple lorsque la présentatrice

vedette américaine Ellen DeGeneres publiait, sur Twitter, un selfie avec onze autres célébrités lors de la cérémonie des Oscars[5]. Certains messages ont conquis la grandeur, tel ce plaidoyer pour des croquettes de poulet qui a finalement obtenu plus de retweets que le selfie d'Ellen DeGeneres. Mais la grandeur s'offre librement à d'autres messages, grâce à une combinaison de coordination, d'amplification inauthentique et de planification méticuleuse. Ces derniers déforment la conversation en ligne et accordent une influence disproportionnée à de petits groupes d'utilisateurs – ce qui est évidemment leur objectif.

L'amplification authentique et inauthentique

De par leur nature, les techniques d'amplification permettent à l'initiateur d'atteindre une audience plus large qu'il ne le pourrait autrement. Mais cela ne veut pas dire que toutes les techniques d'amplification sont malveillantes ou inauthentiques : on peut tout simplement payer pour promouvoir un message, ou coordonner plusieurs utilisateurs humains pour utiliser un mot-clé ou un *hashtag* (un mot-clé précédé par le signe « # », conçu pour être recherché facilement) au même moment. L'amplification devient problématique lorsqu'elle utilise des techniques supposément invisibles voire trompeuses, ou lorsqu'elle déploie un grand nombre de comptes inauthentiques, sans individus réels aux commandes, pour créer un bruit bien plus important que ne le pourraient des utilisateurs humains.

Identifier une amplification authentique d'une amplification inauthentique est un travail délicat. À l'occasion d'une élection sénatoriale partielle dans l'Alabama en novembre 2017, par exemple, des utilisateurs de Twitter soutenant la candidature du démocrate Doug Jones ont coordonné une campagne promouvant le hashtag #DigDoug. Les

organisateurs ont ainsi créé une *tweet sheet*, une liste de tweets que les utilisateurs pouvaient copier, coller et publier, et l'ont automatisée pour permettre à tout individu de simplement cliquer sur un lien de la liste et de voir le message apparaître sur sa page Twitter, prêt à être publié. Ces mêmes organisateurs ont également décidé d'une « heure zéro » à laquelle ils encourageaient tous les soutiens du démocrate à poster simultanément et ainsi former une « tempête Twitter ». Ils ont annoncé publiquement cette initiative sur le réseau Twitter, et il en a résulté une période courte mais intense d'activité : le hashtag rassembla 40 000 tweets, dont un cinquième posté par seulement cinquante comptes très actifs[6].

Il s'agissait bien d'une amplification coordonnée, mais une analyse minutieuse nous apprend que la plupart des comptes étaient bien tenus par des opérateurs humains. La coordination était publique, grâce à un message posté sur le site Twitter. Ainsi, il y avait une volonté d'amplification mais l'effort a été mené par des opérateurs humains, sans tactiques trompeuses.

Cet exemple contraste avec une opération d'amplification inauthentique qui a eu lieu au Mexique en juin 2018. En amont de l'élection présidentielle mexicaine, BuzzFeed News, un média en ligne qui s'intéresse aux sujets à fort potentiel de « buzz », avec un accent particulier sur les questions technologiques, politiques, et sur les réseaux sociaux, a publié un entretien vidéo avec celui qui avait été baptisé le « roi mexicain des *fake news* » : l'opérateur de réseaux sociaux Carlos Merlo[7]. Durant cet entretien, Merlo a montré au journaliste de BuzzFeed comment il avait construit une feuille de calcul (*spreadsheet* : une liste sous forme de tableau) reprenant les tweets promouvant le hashtag #GanaConVictoryLab (« Gagner avec Victory Lab », le nom de son entreprise), au demeurant similaire à celle préparée par les opérateurs de #DigDoug. Mais, au lieu de coordonner ses actions avec des utilisateurs humains, Merlo a utilisé une série de comptes « bots » (un compte automatisé qui publie des messages sans intervention humaine) pour automatiser la publication. L'équipe de BuzzFeed a observé les

prémices d'un « buzz » autour de ce hashtag au Mexique quelques heures plus tard.

Le Digital Forensic Research Lab de l'Atlantic Council (DFRLab) a analysé le trafic sur Twitter et a montré que le hashtag de Merlo avait été mentionné 4 330 fois, par seulement 231 comptes, apparemment tous automatisés[8]. Certains de ces bots avaient également été utilisés auparavant dans d'autres campagnes de soutien à un hashtag, attaquant ou défendant divers candidats lors d'élections mexicaines. Derrière chacun de ces hashtags, on retrouve une explosion soudaine du trafic causée par un petit nombre de comptes publiant très rapidement.

Tout comme pour #DigDoug, #GanaConVictoryLab se distingue par l'utilisation coordonnée d'un petit nombre de comptes très actifs publiant un très grand nombre de tweets, et permettant ainsi d'activer l'algorithme de « tendances » (*trending topics*) de Twitter. Mais, à l'inverse de #DigDoug, #GanaConVictoryLab n'a pas utilisé de comptes humainement opérés, mais des faux comptes automatisés.

Les comptes automatisés (bots)

Des opérations informationnelles peuvent créer une amplification inauthentique de plusieurs manières, rudimentaires ou sophistiquées. L'usage le plus rudimentaire est l'utilisation d'un grand nombre de faux comptes automatisés – bots – pour republier (*retweet*), aimer (*like*), partager ou suivre un message ou un utilisateur spécifique.

Nous avons de nombreux exemples d'amplification liés à l'usage massif de bots, depuis les interventions concomitantes aux débats télévisés lors de la campagne présidentielle américaine de 2016[9] jusqu'à l'amplification du discours anti-vaccination[10]. Certains bots sont utilisés à des fins vraisemblablement politiques, alors que d'autres le sont dans un but

commercial, tels ceux révélés par le *New York Times*, recrutés pour gonfler la liste des abonnés aux comptes de diverses célébrités et d'aspirants à la célébrité[11].

De telles opérations reposant sur des bots sont souvent rudimentaires et faciles à repérer : les bots sont en général privés de photo de profil et d'un nom convaincant, leurs pages n'affichant qu'une liste interminable de retweets, dans un nombre invraisemblable de langues, preuve du marché mondialisé de l'amplification à la demande. Il existe des centaines de milliers de bots de cet ordre. Certains opérateurs, telle l'entreprise américaine dont les activités ont été dévoilées par le *New York Times*, offrent des comptes automatisés plus plausibles, calqués sur des comptes réels existants. Mais, le plus souvent, ces bots se distinguent davantage par leur quantité que par leur qualité.

Les bots sont souvent présentés comme un problème propre à Twitter ; en réalité, un nombre (certes plus réduit) de bots peut être retrouvé sur toutes les plateformes communautaires. Un réseau de faux comptes YouTube a, par exemple, été utilisé pour amplifier des vidéos attaquant les manifestations à Hong Kong durant l'été 2019. Certains de ces comptes publiaient les mêmes vidéos, dans le même ordre, au même moment : un signe révélateur classique du comportement de bots automatisés[12]. Au sein de ce même réseau, on retrouva des comptes Facebook qui fonctionnaient de la même manière. Des bots malveillants ont par ailleurs été repérés sur Reddit (une plateforme numérique où les utilisateurs peuvent librement discuter et partager des contenus divers et variés ; c'est le cinquième site le plus visité aux États-Unis)[13] et dans les pages « commentaires » de blogs[14].

En février 2018, Twitter a annoncé de nouvelles règles pour limiter l'utilisation de bots malveillants, y compris les amplificateurs de masse[15]. Depuis, les « éleveurs » de bots (*bot herders*) ont redoublé d'efforts pour se faire plus discrets, en utilisant un nombre plus restreint de comptes et en lardant ces pages de publications non opérationnelles : les messages conçus

dans le cadre de leurs opérations, que ce soit à des fins politiques ou commerciales, alternent avec d'autres messages en apparence indésirables (*spams*) et sans aucun lien apparent avec la campagne, faisant ainsi office de camouflage. Nous appelons cette utilisation de spams pour cacher l'utilisation opérationnelle d'un compte « spamouflage » ; elle peut être observée sur tous les réseaux sociaux.

Par exemple, un étrange réseau de bots (*botnet*) actif sur Twitter, et apparemment contrôlé par un opérateur commercial russe, attirait les internautes de sexe masculin vers un piège à clics (*clickbait*) pornographique – un site Internet couvert de publicités et conçu pour encourager les utilisateurs à cliquer sur le lien du site et ainsi générer des revenus publicitaires pour son propriétaire – en intercalant des photos de lingerie féminine entre des messages reproduisant automatiquement des extraits du roman *Raison et sentiments* de Jane Austen[16]. Que ces messages aient été automatiquement générés par des bots est facile à prouver : typiquement, une citation commençait et se terminait au milieu d'une phrase du roman, par exemple : « personne d'autre que moi." Elinor sourit, et ». Le compte YouTube mentionné plus haut adjoignait également à ses messages politiques de courtes vidéos de musique, de paysages, de cuisine, ou de chats, la plupart extraites du réseau social chinois TikTok.

Les techniques de camouflage – ou de spamouflage – varient, mais la raison d'être de tels réseaux de bots reste la même : amplifier le message d'un opérateur et faire croire que de nombreux utilisateurs portent un intérêt à ce sujet et soutiennent ses opinions, alors même que, en réalité, un individu ou un petit groupe d'individus sont seuls responsables de ce contenu.

Les types de comptes amplificateurs

Les comptes utilisés pour générer une amplification inauthentique varient beaucoup. Créer un compte sur Twitter a longtemps été facile, et la plateforme permet de créer des comptes qui ne sont pas automatiquement liés à une véritable identité, rendant relativement aisée la création en masse de comptes par des acteurs malveillants. (Lorsque Twitter a accru ses efforts pour empêcher la création de faux comptes, des éleveurs de bots ont apparemment recruté des employés pour industrialiser la création des comptes, sans avoir besoin de l'automatiser[17].)

De son côté, Facebook insiste pour que le propriétaire d'un compte utilise sa véritable identité et impose une vérification avant de pouvoir utiliser tout nouveau compte, y compris la vérification des documents officiels d'identité si jamais le compte est signalé comme suspect. Si ce système n'est pas infaillible, notamment avec les comptes les plus anciens – l'auteur de ce chapitre a déjà rencontré des comptes portant le nom de « Banane », « Café », et même « Ffffff » –, l'amplification de masse utilisant de faux comptes Facebook expressément créés dans cet objectif en devient plus difficile.

Pour contourner cette difficulté, il semblerait que certains opérateurs aient pris le contrôle de comptes d'utilisateurs réels. Le réseau qui a posté des messages en chinois attaquant les manifestants à Hong Kong dénombrait des comptes Facebook apparemment liés à de jeunes Bangladais qui publiaient en bengali avant de brusquement passer au chinois au second trimestre 2019. Un exemple relevé exprime bien la confusion d'un ami du propriétaire d'un compte bangladais qui a commenté un message en chinois par un « Mais qu'est-ce que tu racontes ? » D'autres comptes de ce réseau publiaient en anglais ou en japonais, avant de se tourner vers le chinois.

Certains de ces comptes semblent avoir été détournés par des pirates d'origine inconnue, et vendus aux organisateurs de l'opération visant Hong Kong : les messages publiés dans la langue d'origine dataient de 2017, ou

d’avant, et un long silence s’ensuivit avant le début des publications en chinois. Il existe un marché noir sur Internet de ces comptes dits « âgés » ou « matures »[18]. Certains comptes YouTube du même réseau ont connu un parcours similaire : utilisés en 2017 ou 2018 pour publier de nombreuses vidéos à grande audience, souvent des films ou des séries dans leur intégralité et en plusieurs langues, ils restent silencieux jusqu’au début de l’année 2019, où ils commencent à publier des vidéos en chinois. Ces comptes piratés échappent souvent à la détection pendant de longues périodes, parce que les utilisateurs originaux ont arrêté de les utiliser et ne se rendent pas immédiatement compte du détournement.

Plus troublant encore, certains des comptes Facebook associés à des Bangladais ont changé d’identité au bout de quelques jours seulement, très rapidement donc après leur création[19]. Ce n’est pas typique de comptes piratés, car il est très improbable qu’un compte ait été piraté et détourné si rapidement sans que l’utilisateur original s’en aperçoive. Il est de fait possible que le créateur original ait transféré le contrôle du compte à un acteur tiers, juste après sa création, pour être utilisé lors d’opérations d’amplification inauthentique. C’est une possibilité troublante, car elle réduit le nombre d’indicateurs que Facebook peut utiliser pour identifier un compte comme authentique ou inauthentique.

Vraisemblablement, de tels comptes « autosabordés » ont également été observés sur Instagram. En août 2018, Facebook a démantelé un marché en ligne brésilien qui vendait des pages et des comptes Facebook, Instagram et Twitter, ainsi que des « j’aime ». Ce marché était remarquable par son degré de transparence : les membres du collectif publiaient, sur une page Facebook publique, des captures d’écran des reçus bancaires pour chacune des transactions effectuées[20]. Elle offrait ainsi une vue intéressante du marché de l’amplification inauthentique : 10 000 « j’aime » sur Instagram s’échangeaient pour 60 dollars. On trouve aussi au moins une personne ayant vendu son compte Instagram, avec un nombre d’abonnés notable.

Ce mélange d'activités authentiques et inauthentiques, conçu pour tromper les plateformes et rendre plus difficile l'identification des faux comptes, est accompagné par la multiplication des comptes « cyborgs » (un hybride humain/machine) sur les réseaux sociaux[21]. Ces comptes partagent et aiment automatiquement les messages postés par d'autres utilisateurs, mais les opérateurs se connectent périodiquement pour publier des commentaires personnels, des réponses, ou toute autre indication d'activité humaine. Ils brouillent ainsi la frontière entre actions automatisées et actions humaines et ils sont plus difficilement repérables par les algorithmes de détection et plus délicats à supprimer pour les plateformes, car les messages ne sont pas tous postés automatiquement.

Les comptes cyborgs permettent aux utilisateurs d'augmenter drastiquement la périodicité de leurs messages, mais ils limitent en conséquence le nombre de comptes qu'un seul utilisateur humain peut contrôler car ils requièrent une activité régulière (mais pas forcément fréquente). Ainsi, ils tendent à être opérés seuls ou en petits groupes, et non pas en réseaux de grande ampleur. Le développement des cyborgs est une autre réponse à l'aptitude, et à la volonté croissante des plateformes de sanctionner les réseaux d'amplification ouvertement automatisés.

Percer parmi les tendances majeures

En 2018-2019, une énième tactique pour maquiller de faux comptes a émergé sur Facebook, quoique jusqu'ici sans succès, qui profite des caractéristiques propres à cette plateforme. Sur Facebook, chaque utilisateur doit avoir un compte personnel ; il peut ensuite utiliser ce compte pour créer des « pages » dédiées à une entreprise, à un produit ou à une cause, par exemple. Depuis quelques années, créer un compte personnel sur Facebook demande de plus en plus de temps car la plateforme insiste davantage sur

l’authenticité et elle a démantelé un nombre croissant d’opérations informationnelles.

Certaines opérations informationnelles ont réagi en utilisant un nombre relativement petit de comptes pour créer un très grand nombre de pages. Ces pages apparaissent en fait conçues pour ressembler à celles d’utilisateurs humains, avec un nom et une photo de profil, et ainsi faire croire à un public peu averti qu’il s’agit de comptes personnels. Le réseau hongkongais mentionné plus haut faisait la part belle à des pages qui utilisaient de véritables photos de profil – souvent des photos de célébrités ou liées à des événements récents – et des noms vraisemblables. Ces pseudo-comptes étaient utilisés pour amplifier du contenu, et pour partager et commenter les messages politiques d’autres utilisateurs (mais pas pour du spamouflage). Il est possible que le partage ait été automatisé ; les commentaires semblent bien avoir été rédigés par des opérateurs humains, faisant de ces comptes des cyborgs plus que des bots. Ils ont eu pour conséquence d’augmenter le nombre de partages, de « j’aime » et de commentaires pour chaque message publié, leur donnant une plus grande apparence de légitimité.

Il faut noter, cependant, que les méthodes d’amplification décrites jusqu’ici permettent d’augmenter le volume du trafic lié à un hashtag, une chaîne de texte (*text string* : une phrase courte), un mème (une image alliée à un petit texte conçue pour être facilement partagée sur les réseaux sociaux) mais sans accroître pour autant le nombre d’utilisateurs réels confrontés à ces contenus. Cela s’explique en premier lieu par l’absence d’abonnés humains à ces faux comptes, et ceux qui en ont – tels que ce compte bangladais passé au chinois – laissent généralement leurs abonnés perplexes. Le réseau lié à Hong Kong comptait des dizaines de comptes sur YouTube, chacun publiant un grand nombre de vidéos politiques sans qu’aucune, à quelques exceptions près, ne dépasse une poignée de vues. Beaucoup d’entre elles n’avaient même jamais été visionnées. De la même

manière, les comptes et pages Facebook de ce réseau publiaient beaucoup, mais les seuls comptes interagissant avec ce contenu étaient membres du même réseau, preuve que l'amplification ne permettait pas de sortir de cette bulle.

C'est la raison principale encourageant les opérateurs, sur Twitter principalement, à essayer de faire entrer leurs contenus parmi les sujets « tendances » des plateformes. L'algorithme de « tendances » scanne le trafic à l'échelle locale, nationale et internationale, et pioche parmi les hashtags et les mots-clés qui sont amplement débattus, ou parmi ceux qui commencent à l'être. La plateforme affiche ensuite ces phrases-clés dans un encart dédié sur un côté de l'écran, permettant à tout utilisateur connecté dans la région de voir, en temps réel, ce dont les autres utilisateurs de cette même région débattent. Lorsqu'une phrase, ou un hashtag, est reprise par cet algorithme, elle s'affiche à beaucoup d'autres utilisateurs géographiquement proches même s'ils n'ont pas auparavant montré de l'intérêt pour ce sujet, et même s'ils ne suivent aucun compte associé à cette phrase. Percer dans cette liste de « tendances » est ainsi le meilleur moyen pour une opération informationnelle d'atteindre des utilisateurs jusque-là non affiliés ; pour cette raison, l'opérateur mexicain précédemment cité insistait tout particulièrement sur sa capacité à piéger l'algorithme de « tendances » de Twitter.

La manipulation experte : le cas de la France

Percer dans cette liste de tendances n'est pas aussi simple que d'allumer un botnet (un réseau de centaines ou de milliers de bots, tous programmés pour accomplir la même tâche) : la manipulation des algorithmes de tendances est un élément central des opérations informationnelles depuis

des années[22], et les plateformes résistent de ce fait aux tentatives les plus flagrantes.

La campagne présidentielle française de 2017 a été l'objet d'une tentative particulièrement habile de déjouer l'algorithme de tendances de Twitter, et avec succès pour ce groupe d'opérateurs apparemment ; ils ont publié périodiquement des captures d'écran des principales tendances en France, leurs hashtags étant systématiquement parmi les trois premières[23]. Ce groupe a combiné des comptes humains, cyborgs et des bots pour créer l'apparence d'un trafic naturel de grande ampleur – jusqu'à 45 000 tweets en moins de deux heures. Cet exemple réussi d'amplification mérite une étude de cas, mais elle souligne également l'ampleur des efforts nécessaires pour arriver à un tel succès.

L'objectif de ce groupe était de faire entrer des hashtags favorables à la candidate Marine Le Pen dans la liste de tendances : les organisateurs ont lancé chaque hashtag avec un appel explicite tel que « Mobilisez-vous sur ce hashtag ! ». La première étape était d'établir un stock de mèmes affichant le hashtag, le nombre variant d'une douzaine à plus de cent. Puis les principaux comptes du groupe commençaient à publier ces mèmes à une « heure zéro » prédéterminée, avec quatre à six comptes publiant chaque hashtag à la même seconde, mais avec différents mèmes et différents textes. Il pouvait s'agir d'une action menée physiquement ou automatiquement préprogrammée. Les principaux comptes continuaient ensuite à publier différents mèmes et textes toutes les cinq minutes, grossissant encore le stock de contenus originaux.

Au même moment, une douzaine d'autres comptes commençaient à republier les principaux messages, avec les mêmes mèmes accompagnés de messages personnalisés, puis à se republier entre eux. Ces comptes secondaires étaient vraisemblablement au moins en partie opérés manuellement : les tweets arboraient un contenu original et ils publiaient à un rythme bien moindre. Cependant, ils ont eu pour effet d'augmenter

considérablement et rapidement le nombre de messages relayant chaque hashtag, et avec suffisamment de variété dans les contenus et dans les images pour laisser penser à un trafic naturel.

Dans un troisième temps, un grand nombre de bots republiaient tous les messages des comptes principaux et tous les tweets et retweets des comptes secondaires. Certains publiaient également les mèmes préparés en amont avec le hashtag de chaque campagne mais sans texte supplémentaire. L'activité de ces bots gonflait grandement le volume total de contenus tout en maintenant un certain degré d'originalité (retweets, images publiées, textes publiés). Cette opération d'amplification demeure la plus réussie jamais observée par l'auteur de ce chapitre.

Le groupe français a rapidement réussi à faire entrer ses hashtags dans la liste de tendances. Malgré tout, il a laissé une signature dans le flux de data qui l'a révélé comme différent d'un flux réellement organique. Et cette même signature montre bien la vulnérabilité fondamentale de toute opération d'amplification (même la plus complexe) : sans avoir une base solide d'utilisateurs humains pour promouvoir leurs contenus, ils doivent nécessairement construire l'apparence d'un intérêt général à travers des dizaines de milliers de messages. Ils ont alors le choix d'utiliser un petit nombre de comptes opérés humainement pour publier à des fréquences très importantes ou un très grand nombre de comptes automatisés qui publient et republient à une fréquence moins importante, parfois une combinaison des deux ; mais chaque méthode laisse des traces lorsque l'on se penche sur les chiffres du trafic total.

Si l'opération utilise un petit nombre de comptes hyperactifs, le nombre total de messages publiés sera impressionnant, mais le nombre moyen de messages par utilisateur sera très largement supérieur à une moyenne naturelle. Ici, nous pouvons prendre l'exemple d'un réseau de bots en Inde qui a amplifié un hashtag du parti BJP au pouvoir et généré 30 000 tweets depuis 50 comptes, pour une moyenne individuelle invraisemblable de 600

messages en quelques heures seulement. Si une opération utilise un grand nombre de bots pour republier des contenus, le volume total de tweets sera substantiel, mais le pourcentage de retweets sera bien supérieur à celui d'un trafic normal. Là, nous pouvons citer un hashtag en soutien au régime saoudien dans sa querelle avec le Qatar qui était tellement trafiqué que 95 % des publications étaient des retweets.

Ces chiffres permettent de calculer dans quelle mesure un hashtag a été amplifié artificiellement sur Twitter[24]. En combinant le pourcentage de retweets, le nombre moyen de tweets par utilisateur, et la proportion du trafic générée par les 50 utilisateurs les plus actifs, on peut attribuer un score numérique à un flux d'information sur Twitter : le coefficient de manipulation du trafic (CMT). Des analyses initiales montrent qu'un flux naturel atteint typiquement un score inférieur ou égal à 12, alors qu'un flux en grande partie manipulé peut facilement multiplier ce résultat par deux. Le cas indien mentionné plus haut offre un CMT de 123,98, le plus haut score jamais mesuré[25]. Les exemples français se situent, malgré un degré certain de sophistication, entre 38 et 53. Ils ont effectivement réussi à tromper l'algorithme de Twitter, mais en laissant des traces derrière eux.

*

Les réseaux sociaux donnent une voix à ceux qui n'en ont pas. Les techniques d'amplification artificielle présentées ici cherchent à produire une voix démesurément forte en utilisant des comptes faux, volés ou automatisés. Ces efforts déforment le trafic en ligne, et peuvent déformer les fondations d'un débat démocratique en permettant à de petits groupes d'apparaître démesurément forts et influents.

Le mot-clé ici est « peuvent ». Les plateformes de médias sociaux ne sont pas sans défenses, et elles ont un intérêt à empêcher de petits groupes d'individus de manipuler leurs algorithmes avec des comptes faux et volés. Il faut d'ailleurs déployer de gros efforts et une technicité certaine pour

neutraliser les défenses de ces plateformes. Cela dit, un utilisateur régulier de ces réseaux peut identifier de lui-même les traces de ces manipulations, en cherchant les comptes qui changent brutalement de langue et de sujet de discussion sans explication. Les plateformes et les chercheurs en open-source peuvent étudier le trafic plus précisément. Comme l'exemple de Hong Kong le montre, c'est une chose que de créer un réseau de faux comptes et de commencer à publier, mais c'en est une autre que de rendre ce contenu visible aux véritables utilisateurs humains.

Lorsque l'on est aux prises avec la manipulation des réseaux sociaux, il est important d'être vigilant, mais également de ne pas exagérer l'impact de l'amplification en ligne. Quelle que soit la forme prise par l'opération informationnelle, c'est l'effet et non l'effort qui compte. Même si les comptes artificiels peuvent faire beaucoup de bruit sur les réseaux, c'est le nombre d'utilisateurs qui entendent ce bruit qui est le plus important. Et c'est un défi majeur pour les chercheurs que de mesurer combien d'utilisateurs humains ont été confrontés aux contenus d'une opération, en regardant au-delà des mesures de base telles que les « j'aime » et les partages, qui ne permettent pas de distinguer les comptes authentiques des comptes inauthentiques.

Pour aller plus loin

ALEKSEJEVA Nika, ANDRIUKAITIS Lukas, BANDEIRA Luiza, BAROJAN Donara, BROOKIE Graham, BUZIASHVILI Eto, CARVIN Andy, KARAN Kanishk, NIMMO Ben, ROBERTSON Iain et SHELDON Michael, « Operation secondary infektion », *Atlantic Council*, juin 2019. Voir https://www.atlanticcouncil.org/in-depth-research-reports/report/operation-secondary-infektion.

NIMMO Ben, « Backdating the blame. How Russia made NATO a party to the Ukraine conflict », Riga, NATO Strategic Communication Center of

Excellence, septembre 2016. Voir https://www.stratcomcoe.org/backdating-blame-how-russia-made-nato-party-ukraine-conflict-author-ben-nimmo.

NIMMO Ben, « Vilify and amplify : How the Kremlin's disinformation machine is attacking the MH17 probe », Stopfake.org, 28 septembre 2016. Voir https://www.stopfake.org/en/vilify-and-amplify-how-the-kremlin-s-disinformation-machine-is-attacking-the-mh17-probe.

NIMMO Ben, « Measuring traffic manipulation on Twitter », Oxford Internet Institute, janvier 2019.

FRANÇOIS Camille, NIMMO Ben, *The IRACopyPasta Campaign*, *Russian Accounts Posing as Americans on Instagram Targeted Bothsides of Polarizing Issues Ahead of the 2020 Election*, New York, Graphika, octobre 2019.

FOCUS 3

Les preuves de la manipulation de l'information

Rémi Géraud-Stewart

> « Photographers, especially amateur photographers, will tell you that the camera cannot lie. This only proves that photographers, especially amateur photographers, can, for the dry plate can fib as badly as the canvas on occasion[1]. »
>
> (Abraham Lincoln, 1895)

Comment reconnaître qu'un article, une image, un enregistrement audio, sont en fait les outils d'une campagne d'influence ? En complément d'une analyse géopolitique et stratégique, il existe des approches scientifiques et techniques que nous proposons ici de discuter. Certaines, issues de l'expertise scientifique, sont déjà utilisées lors d'enquêtes judiciaires pour confondre les tentatives d'altérer des éléments de preuve. D'autres n'ont pas leur pendant forensique[2], mais permettent de faire la lumière sur les techniques et objectifs des organisateurs de ces campagnes de guerre informationnelle. Il s'agit donc de collecter un faisceau

d’éléments, en ayant à l’esprit les outils disponibles pour créer des faux ou tromper avec du vrai.

Reconnaître le faux

L’enquête est généralement menée sur trois fronts :

- *le contenu* : analyser l’état actuel d’un document ;
- *l’historique* : reconstruire à partir de traces l’historique qui a amené à cet état ;
- *le contexte* : confronter avec d’autres éléments environnants.

Si le contenu est en principe donné, il faut parfois fournir de gros efforts pour reconstruire l’historique et préciser le contexte de l’objet analysé. Le résultat de ces deux enquêtes est souvent au mieux fragmentaire et hypothétique. Par exemple, l’étude de faux photographiques se fait en recherchant un original (dont le faux serait dérivé et dont on pourrait assurer l’antériorité), des marqueurs de manipulation dans l’image ou d’autres prises de vues de la même scène (confirmant ou confrontant le cliché incriminé).

Parmi les marqueurs de manipulation courants, on trouve notamment les erreurs de perspective, les erreurs de luminosité (éclairage, réflexions, ombres), les désaccords de compression (images assemblées à partir de plusieurs sources), la duplication (augmentation artificielle du nombre de missiles, de véhicules, etc.), le flou et d’autres distorsions d’origine non optique, les discontinuités de flot optique (liées au *tracking*[3]) et les métadonnées[4]. Chaque marqueur correspond à une technique d’altération connue, et, dans une large mesure, les outils engagés ici par l’analyse recoupent ceux utilisés par le renseignement traditionnel.

Cette manière de faire n’est pas infaillible, car la désinformation ne se limite pas aux faux. Il est possible, par exemple, de diffuser des images

authentiques, mais tirées d'un contexte différent de celui discuté (des mouvements de troupes réels, mais dans un autre pays), ou de n'en montrer qu'un extrait, dans l'intention de tromper. Le cas le plus courant est sans doute le mélange, en proportions variables, d'éléments véridiques et d'éléments altérés, voire inventés : le destinataire est mis en confiance par les premiers pour admettre les seconds.

Pour ajouter à la difficulté, l'accès démocratisé depuis quelques années aux techniques génératives (*deep fakes*, *inpainting*, rendu 3D) et de post-production permet avec peu de moyens de produire des images, vidéos et sons réalistes. Ces contrefaçons ont un pouvoir de conviction fort, surtout dans un contexte d'échanges informels. Les *deep fakes* consistent à altérer une partie d'une image, typiquement le visage d'une personne, en s'appuyant sur des techniques d'apprentissage statistique pour y placer le visage d'une autre. La détection de visage et son remplacement de façon ajustée sont automatiques, donc accessibles en principe au plus grand nombre, contrairement aux approches traditionnelles qui nécessiteraient des compétences en traitement d'image.

De telles techniques sont toutefois aujourd'hui limitées : les *deep fakes* nécessitent entre autres de nombreuses prises de vue pour en synthétiser une nouvelle, ce qui restreint leur utilisation à des célébrités très médiatisées. Pour la même raison, remonter à un original est relativement aisé, des outils de reconnaissance ayant été créés et mis à disposition du public par des entreprises spécialisées, comme TinEye[5], et par l'association de défense des droits de l'homme Amnesty International (CitizenEvidence[6]). Il existe même des outils spécialisés capables d'identifier le faux et la méthode employée comme FaceForensics[7], participant avec d'autres au défi de détection des hyper-trucages (*Deepfake Detection Challenge*)[8].

Reconnaître le vrai

Cette capacité à créer des faux qui ressemblent à s'y méprendre à des documents authentiques renverse en fait la charge de la preuve : qu'est-ce qui permet d'étayer l'authenticité d'une information ? En effet, si une incohérence, que ce soit dans l'historique, le contenu ou le contexte, révèle une possible manipulation, l'absence d'incohérence n'est pas en soi une preuve de vérité. Rares sont les clichés signés numériquement par leur auteur, ce qui constituerait une preuve pratiquement inaltérable.

On s'appuie plutôt dans ce cas sur trois heuristiques : la présence datée de copies de l'objet incriminé chez des tiers, provenant d'une autre source ; la présence de versions plus longues chez des tiers ; la haute qualité de l'objet analysé. On suppose en effet qu'il est plus facile d'extraire un morceau d'image ou de vidéo que de l'étendre. La présence d'une version plus longue révélerait alors un extrait ou une modification par rapport à un original, *a minima* un recadrage, par exemple pour éviter un logo.

Concernant la troisième heuristique, la mauvaise qualité d'image, la surcompression, le mauvais éclairage, la désaturation, le cadrage très agité, etc., sont des méthodes classiques pour dégrader la lisibilité et dissimuler des manipulations opérées sur l'image.

Ces critères ne sont pas limités aux images et aux sons, ils s'appliquent également aux extraits de texte. Ainsi la citation placée en exergue et attribuée à Lincoln se retrouve *verbatim* dans plusieurs publications, datées de 1895. L'article dont elle est tirée est bien plus long, néanmoins on pourra s'assurer qu'en contexte la citation ne trahit pas l'auteur. Enfin, le texte ne souffre pas des altérations liées à la compression des sons ou des images.

Reconnaître l'influence par ses objectifs

Malheureusement, les méthodes d'investigation mentionnées ci-dessus prennent du temps et s'adressent d'abord à un juge ou à un expert ; elles

supposent également un effort concentré sur un objet en particulier. De plus, elles aboutissent souvent à une conclusion mitigée : il n'y a pas de trace indiscutable de faux, mais il n'y a pas non plus de trace indiscutable de vrai.

Pour surmonter cette aporie, on peut s'intéresser à ce qui motive l'influence, en cherchant ses symptômes. L'un d'entre eux est la diffusion qui est poussée par des stratégies semi-automatisées et dont on peut parfois identifier l'origine[9]. Un autre angle s'appuie sur le contenu des messages de désinformation, qui vise à produire un effet psychologique sur les populations-relais. De tels effets sont évidemment difficiles à mesurer de façon automatisée, mais quatre d'entre eux se prêtent relativement bien à un exercice de ce type :

- la confusion, causée par la coexistence de nombreuses versions discordantes d'un même sujet. Par exemple, à propos des empoisonnements de Salisbury, plusieurs médias dans la sphère russophone ont mis en avant des versions accusant tour à tour le Royaume-Uni, la Géorgie, l'Iran d'être les commanditaires ;
- le *priming*, un procédé qui consiste à diffuser une première version délibérément mensongère, avant de la retirer, le démenti ayant toujours moins d'impact que le message d'origine et finissant par être oublié. Par exemple, l'attaque sur la chaîne TV5 Monde en 2015 a initialement été attribuée à un groupe jihadiste. Bien qu'on sache aujourd'hui que cette attribution était prématurée et erronée, de nombreux médias la relatent encore ;
- l'indignation, dont les effets neurophysiologiques sont prévisibles et documentés[10] et qui se caractérise par des temps de réaction raccourcis et un autorenforcement : les groupes concernés deviennent de plus en plus suggestibles à ces types de tactiques (certains traits peuvent être identifiés par l'analyse automatisée de textes) ;
- l'effet de volume, causée par la diffusion simultanée de plusieurs versions concourantes d'un même discours et par l'appui de méthodes

d’amplification, donnant une impression factice de consensus.

En jouant sur ces différents mécanismes psychologiques, les coordinateurs d’une campagne de désinformation cherchent non seulement à diffuser leur message, mais aussi à créer les conditions d’une diffusion future. L’intérêt pour l’analyste est qu’il est possible d’effectuer un traitement statistique « en masse » à la recherche de ces indicateurs, à des échelles de temps relativement courtes.

La question de la « source »

Ayant établi la réalité d’une opération d’influence, une question courante est de remonter à ses organisateurs. Ici encore l’analyse des enjeux géopolitiques peut être complétée par des observations techniques. On s’intéresse, par exemple, aux moyens investis par les coordinateurs (production, logistique de diffusion, suivi) pour estimer le nombre de personnes impliquées. On s’intéresse également aux métadonnées explicites, comme les tags de géolocalisation[11], mais aussi implicites, comme les paramètres optiques d’une caméra. On s’intéresse enfin aux chemins par lesquels l’information est parvenue à ses cibles. Les objectifs généraux, les méthodes, les moyens constituent un profil susceptible de se conserver d’une opération à l’autre.

Cela ne signifie pas pour autant que l’on puisse attribuer un profil à un acteur déterminé[12]. D’une part, l’automatisation démultiplie le pouvoir de peu d’individus. D’autre part, les métadonnées peuvent être modifiées délibérément. Sur le plan technique, il existe donc toujours un déni plausible, exacerbé par la visibilité imparfaite de l’analyste sur les moyens de diffusion existants.

Une autre raison qui explique l’impossibilité d’engager une attribution est la prévalence de *prestataires*, spécialisés dans des opérations d’influence

et missionnés par des groupes différents aux intérêts parfois contradictoires. Établir raisonnablement le profil du prestataire relève encore du domaine technique, mais remonter aux *commanditaires* ne l’est généralement pas.

II

LES GUERRES DE L’INFORMATION EN CONTEXTE AUTORITAIRE

CHAPITRE 4

La Russie : « l’espace informationnel » comme terrain de conflictualité

Maxime Audinet et Céline Marangé

Les actions de type informationnel peuvent s’exercer dans différents cadres, être de type médiatique ou cybernétique, s’inscrire dans des opérations de coercition, d’influence ou de persuasion. Elles n’en sont pas moins pensées et analysées en fonction de représentations spatiales et sémantiques qui varient selon les pays et les cultures stratégiques. Certains pays mettent l’accent sur le contenu de l’information, quand d’autres s’intéressent plutôt aux systèmes numériques d’échange de données.

En Russie, on emploie le concept d’« espace informationnel » (информационное пространство) dans les discours publics et les documents de doctrine, là où, dans les pays occidentaux, la notion de « cyberespace » est volontiers mobilisée. Plus qu’une différence de terminologie, cette distinction traduit une différence d’approche. Le terme occidental de « cyberespace » renvoie au medium, c’est-à-dire au système cybernétique de diffusion de l’information. Par extension, il qualifie les médias en ligne et les réseaux sociaux, tout en excluant les médias classiques. Le terme russe d’« espace informationnel » est plus extensif : il

désigne tant le contenu diffusé que le contenant par lequel l'information transite[1]. Il sert, en réalité, à qualifier un espace virtuel qui constitue un terrain de conflictualité, comme des espaces géographiques réels, sur terre, sur mer, dans les airs et dans l'espace.

Les autorités russes affirment que la « souveraineté informationnelle » doit être protégée au même titre que l'intégrité territoriale. La préservation de « l'espace informationnel » russe implique des actions défensives et offensives. Celles-ci s'appliquent aux contenants afin de protéger les infrastructures critiques d'éventuelles cyberattaques ou d'attaquer celles de l'adversaire ; elles visent aussi les contenus afin de préserver son « espace informationnel » d'actions extérieures malveillantes ou de porter atteinte à celui de l'adversaire.

Cette vision fondamentalement défensive de l'information n'empêche pas la mise en œuvre d'une politique d'influence ouverte, ni le recours à des actions offensives secrètes. L'outil informationnel est désormais pleinement intégré à la stratégie de politique étrangère et à la planification militaire. Par le biais de l'Administration présidentielle, des ministères des Affaires étrangères et de la Défense et des « structures de force[2] », l'État russe a réussi en l'espace d'une décennie à mettre des technologies modernes au service d'une conception de l'information encore largement héritée de la période soviétique.

Une vision défensive de l'information

Plusieurs textes officiels définissent l'action de la Russie dans cet « espace informationnel ». Produits par le Conseil de sécurité de la Fédération de Russie, le ministère de la Défense et le ministère des Affaires étrangères, puis adoptés par décret présidentiel, ces documents de doctrine présentent une cohérence d'ensemble et donnent une image avant tout

défensive et sécuritaire de l'action informationnelle de la Russie. L'objectif revendiqué est de contrôler l'information afin d'étendre la souveraineté nationale au domaine de l'information et de protéger la population russe contre des menaces informationnelles extérieures.

L'information comme composante de la sécurité nationale

La première doctrine de sécurité de l'information de la Fédération de Russie (Доктрина информационной безопасности РФ) date du mois de juin 2000, quelques mois après l'arrivée au pouvoir de Vladimir Poutine. Dès le début de son mandat, le Kremlin prend des mesures de restauration d'un « État fort » et de reprise en main d'un certain nombre de secteurs-clés, y compris dans le champ informationnel et médiatique[3]. Ce texte, le premier du genre, a été préparé par le Conseil de sécurité : une première ébauche a été rédigée en 1994, mais le texte est approuvé sous la direction de Sergueï Ivanov (1999-2001), l'ancien directeur adjoint de Vladimir Poutine au FSB (1998-1999)[4].

La seconde et dernière doctrine en date a été adoptée en décembre 2016, dans un contexte marqué par la guerre en Ukraine et l'intervention armée russe en Syrie. Il s'agit, selon ses auteurs, d'un « document de planification stratégique » visant à étendre les principes directeurs de la stratégie de sécurité nationale de 2015 dans le but de protéger les « intérêts nationaux [du pays] dans la sphère informationnelle » (art. 8). La sécurité de l'information y est définie comme « la protection de l'individu, de la société et de l'État contre des menaces informationnelles intérieures et extérieures, afin de garantir les droits humains et les libertés civiles […], la souveraineté, l'intégrité territoriale et le développement socio-économique de la Fédération de Russie, la défense et la sécurité de l'État » (art. 2.в)[5].

La doctrine de sécurité de l’information présente une typologie des « menaces informationnelles » et révèle comment les dirigeants russes conçoivent leur nature et leur acuité (section 3). D’un côté, elle donne une vision assez classique et consensuelle des défis posés par le développement d’Internet : le texte pointe les dangers que représentent la criminalité informatique dans le domaine financier (art. 14) et les cyberattaques contre des infrastructures critiques à des fins militaires et politiques (art. 15 et 16) ; il met en garde contre l’utilisation des technologies numériques par des groupes terroristes pour attirer de nouvelles recrues, inciter à la haine et polariser la société russe (art. 13).

D’un autre côté, cette doctrine épouse le discours officiel russe sur l’environnement stratégique et la compétition internationale en inscrivant les menaces informationnelles dans des rivalités de puissance. Elle préconise, en particulier, de réduire la « dépendance » des industries numériques russes à l’égard des technologies étrangères (art. 17) ; elle accuse les « médias étrangers » de publier des « contenus biaisés sur la politique de l’État russe » et de chercher à influencer la population russe, « notamment la jeunesse, afin d’éroder les valeurs morales et spirituelles traditionnelles », désignant à mots couverts les pays occidentaux (art. 12). Enfin, cette doctrine reproduit certains poncifs soviétiques en soulignant le danger que représente « l’influence psychologique et informationnelle » de services de renseignement étrangers, de groupes religieux ou d’organisations de défense des droits de l’homme à des fins de déstabilisation intérieure (art. 12).

L’idée qu’il faut combattre « les diversions idéologiques inspirées depuis l’étranger » n’est pas nouvelle. Cette obsession des dirigeants soviétiques entraîna les purges staliniennes, qui anéantirent des millions de personnes accusées d’appartenir à des réseaux d’espions étrangers ou à des cercles trotskistes. Elle justifia aussi la création de la Cinquième Direction du KGB en 1967 à la demande de son chef, Iouri Andropov. Pour appuyer

sa demande, Andropov soulignait le rôle que les États-Unis attribuaient à la « guerre psychologique » (психологическая война) dans la lutte contre le communisme[6]. Cette direction avait pour mandat de démasquer et de mettre en échec les opérations des services secrets et des centres antisoviétiques à l'étranger dans le domaine de la « lutte idéologique », tout en détectant « les phénomènes malsains dans certaines couches de la population pouvant être exploités par l'adversaire à des fins de sape »[7].

L'information comme vecteur de diplomatie publique

Comme à l'époque soviétique, la Russie utilise l'information comme un instrument de rayonnement et d'influence. Dans ce domaine, le ministère des Affaires étrangères joue un rôle prépondérant. Il définit les orientations en matière d'information dans sa doctrine de politique étrangère (Концепция внешней политики РФ). Celle de 2008, entérinée moins d'un mois avant la guerre des cinq jours avec la Géorgie, affirme le rôle de l'information comme outil privilégié de diplomatie publique. L'objectif affiché est d'accroître l'attractivité de la Russie dans le monde et de redonner du lustre à son image écornée :

> Dans le cadre de sa diplomatie publique, la Russie va chercher à donner une image objective d'elle-même dans le monde, à développer ses propres moyens d'influence informationnelle vis-à-vis de l'opinion internationale, à assurer le renforcement de la place des médias de masses russes dans l'espace informationnel mondial en leur fournissant le soutien indispensable de l'État, à participer activement à la coopération internationale dans le domaine de l'information et à prendre les mesures nécessaires pour répondre aux menaces informationnelles [qui portent atteinte] à sa souveraineté et à sa sécurité[8].

Forgé au début des années 1990 par le théoricien américain des relations internationales Joseph Nye, le concept de *soft power* désigne « la capacité à obtenir ce que l'on veut par l'attraction plutôt que par la coercition et la rétribution[9] ». Il apparaît en Russie au milieu des années 2000, après la traduction en russe de l'ouvrage de Nye, *Soft Power*, en 2004. L'expression russe correspondante (мягкая сила ou force douce) reste d'abord confinée aux cercles universitaires. Le ministre des Affaires étrangères Sergueï Lavrov l'a employée pour la première fois en 2008, dans une perspective proche de celle de Nye, pour défendre l'idée qu'il fallait doter la Russie de ce nouvel attribut de puissance qui lui permettrait de soutenir la comparaison, de gagner en influence et d'accroître son attractivité[10].

Toutefois, les élites politiques russes donnent une interprétation ambivalente du *soft power* à partir de 2012[11]. Le discours russe sur le *soft power* sert dès lors à qualifier la politique d'influence occidentale, jugée subversive et déstabilisante, à l'origine des « révolutions de couleur » d'essence libérale survenues dans l'espace post-soviétique[12]. Vladimir Poutine s'empare du terme au lendemain des printemps arabes et des grandes manifestations de l'hiver 2011-2012. En campagne pour un troisième mandat présidentiel, il publie un manifeste qui atteste cette représentation négative :

> La notion de *soft power* est employée de plus en plus fréquemment […]. Malheureusement, ces méthodes sont trop souvent utilisées […] pour manipuler l'opinion et pour intervenir directement dans la politique intérieure de pays souverains. Il faut clairement distinguer la liberté d'expression et une activité politique normale, d'une part, et, d'autre part, les instruments illicites du *soft power*. On ne peut que saluer le travail civilisé des ONG humanitaires et caritatives, y compris celles qui critiquent activement les pouvoirs en place. Toutefois, pour ce qui concerne les « pseudo-ONG » […] dont le

but est de déstabiliser la situation de tel ou tel pays avec un soutien étranger, leurs activités sont inacceptables[13].

Dans le même temps, le Kremlin reconnaît une valeur instrumentale au *soft power*. Juste après sa réélection en 2012, Poutine demande au corps diplomatique d'œuvrer en faveur de l'image du pays : « L'image de la Russie à l'étranger n'est pas forgée par nous, déclarait-il, si bien qu'elle est souvent déformée ou qu'elle ne reflète pas la situation réelle du pays ou la contribution de la Russie à la civilisation[14]. » La doctrine de politique étrangère de 2013 compare le *soft power* à « une boîte à outils complète qui vise à accomplir des objectifs de politique étrangère […] par des méthodes et des technologies alternatives à la diplomatie traditionnelle[15] ». Celle de 2016 insiste sur la nécessité de propager par ces vecteurs « le point de vue russe sur les processus internationaux » et de renforcer la compétitivité de la Russie dans l'environnement médiatique global[16].

L'information comme terrain de rivalité mondiale

Au moment de l'annexion de la Crimée, qui marque l'acmé des tensions avec les pays occidentaux, les rivalités s'exacerbent et reconditionnent le rapport des élites russes à l'information. Une thèse fait alors quasiment l'unanimité à Moscou, tant au sein des milieux de la défense que dans les débats télévisés diffusés aux heures de grande écoute : une « guerre de l'information » (информационная война) opposerait au niveau mondial la Russie, comme l'Union soviétique en son temps, à « l'Occident » (Zapad), présenté comme une entité homogène. La Russie serait en butte à une guerre non déclarée de « l'Occident » et, en particulier des États-Unis, qui l'attaqueraient par le truchement des sanctions économiques, des pressions diplomatiques et de « l'arme de l'information », afin de provoquer un changement de régime à Moscou, voire d'entraîner un nouveau

démembrement du pays. Bien que la notion de « guerre de l'information », dont le caractère sensationnaliste peut paraître incompatible avec la rigueur des doctrines, ne soit jamais utilisée dans les documents stratégiques officiels, de hauts responsables de l'État, comme le chef de l'Administration présidentielle Sergueï Ivanov, endossent cette idée[17].

Celle-ci ne date toutefois pas de la crise ukrainienne. À l'époque soviétique, la « guerre de l'information » était une discipline enseignée. Introduite pour la première fois en 1942 à l'Institut militaire des langues étrangères, elle a été supprimée des programmes dans les années 1990 et réintroduite dans les années 2000. La notion de « guerre de l'information » est alors popularisée par quelques politistes ayant reçu leur formation et commencé leur carrière au KGB. Ainsi en est-il d'Igor Panarin, doyen de l'Académie diplomatique et figure médiatique. Dans un ouvrage intitulé *La Deuxième Guerre mondiale de l'information est une guerre contre la Russie*, il écrit que les Printemps arabes et les manifestations de décembre 2011 à Moscou résultent d'une agression américaine et accuse les États-Unis de se servir des technologies de l'information pour influencer et manipuler les opinions publiques étrangères[18]. Vladimir Novikov, auteur de *L'Arme de l'information. Une arme des guerres présentes et futures*, distingue quatre scénarios de « guerres de l'information ». Le premier consiste à créer « dans le pays une situation révolutionnaire menant à un changement de pouvoir sans intervention d'une armée extérieure et sans occupation du territoire[19] ».

Ces thèses entrent en résonance avec les réflexions sur l'évolution des formes de conflictualité et le rôle des opérations d'information dans les guerres contemporaines, présentées dans un article de 2013 par le chef d'état-major de l'armée russe Valeri Guerassimov. Sans être une doctrine[20], ce texte éclaire la manière dont les responsables militaires russes conçoivent l'utilisation de l'information à des fins stratégiques et dans la planification opérationnelle.

> On observe au XXIe siècle une tendance à l'effacement des distinctions entre l'état de guerre et l'état de paix. Les guerres ne sont plus déclarées, et, une fois commencées, se déroulent suivant un modèle qui ne nous est pas familier. […]
> Les « règles de la guerre » mêmes se sont considérablement transformées. Les moyens non militaires ont vu leur rôle s'accroître pour atteindre des objectifs stratégiques et politiques, et, dans de nombreux cas, dépassent de loin par leur efficacité la force des armes. Les méthodes de lutte utilisées mettent désormais l'accent sur une large (gamme) de moyens politiques, économiques, informationnels, humanitaires, ainsi que sur d'autres moyens non militaires, réalisés par l'implication du potentiel de protestation de la population. […]
> Les actions asymétriques se sont largement diffusées, permettant de niveler la supériorité de l'adversaire dans le conflit armé. S'y rapporte le recours aux forces d'opérations spéciales et à l'opposition intérieure pour créer un front perpétuellement actif sur tout le territoire de l'État adverse ; [s'y rapporte également] une action informationnelle dont les formes et les moyens se perfectionnent en permanence[21].

Étant donné l'importance accordée à l'information dans les conflits contemporains et la dangerosité des intentions prêtées à l'adversaire, il n'est pas surprenant que cette « guerre de l'information » appelle des actions résolues. Ainsi les dirigeants russes appuient leur posture défensive en associant des moyens défensifs, tels que la défense de la « souveraineté numérique[22] » et le renforcement du contrôle d'Internet, et des moyens offensifs, comme l'espionnage, la désinformation, les cyberattaques et la destruction des systèmes d'information.

Un large spectre d’actions offensives

L’action informationnelle de la Russie répond avant tout à des visées sécuritaires, celles de protéger le pays et le régime politique contre toute intrusion extérieure. Elle ne saurait toutefois se réduire à une stratégie purement défensive. Les doctrines et les pratiques révèlent une ambition assumée, celle d’exercer une influence informationnelle dans le monde et de répondre aux attaques dont la Russie serait victime dans le domaine médiatique. Cette influence se décline sur un large spectre et donne lieu à des actions offensives de différentes natures. Elle s’étend du *soft power*, exercé par la diplomatie publique et les médias, au *hard power*, qui se traduit par des cyberattaques, des opérations de subversion, voire par la possibilité de mener des attaques physiques destinées à empêcher la capacité de communication et d’information d’un adversaire. En fonction des domaines concernés et des actions considérées, différents acteurs institutionnels sont impliqués.

Le recours à des médias d’influence « alternatifs »

L’audiovisuel extérieur public représente le principal instrument officiel de la diplomatie publique et le versant le plus ouvert de l’influence informationnelle de la Russie. RT et Sputnik sont deux structures distinctes sur un plan institutionnel, mais complémentaires dans leur ligne éditoriale qui se veut « alternative » aux médias dominants occidentaux (*mainstream media*). La première chaîne anglophone de Russie, alors appelée Russia Today, est créée en juin 2005 à l’initiative de l’agence RIA Novosti. Le projet est sorti des tiroirs du ministère de la Presse en réaction à la Révolution orange de 2004 en Ukraine, d’inspiration pro-européenne. En coulisse, deux personnalités proches des plus hautes instances du pouvoir ont œuvré au lancement de RT : il s’agit de Mikhaïl Lessine, l’ancien

ministre de la Presse (1999-2004) et conseiller pour les médias des présidents Poutine et Medvedev (2004-2009), et d'Alekseï Gromov, alors porte-parole du Kremlin (2000-2008) et actuel premier directeur adjoint de l'Administration présidentielle. Ce dernier confie en 2005 la rédaction de RT à Margarita Simonian, une jeune journaliste de 25 ans, ancienne correspondante au « pool du Kremlin », le groupe des journalistes accrédités pour suivre le président.

En décembre 2013, Vladimir Poutine décrète la dissolution de RIA Novosti et de la radio La Voix de la Russie, dans le cadre d'une réforme controversée de l'audiovisuel public, officiellement pour des raisons budgétaires. Gromov et Lessine (alors directeur de la holding Gazprom-Media) sont à nouveau à la manœuvre. Lors de cette reprise en main par l'État, RIA Novosti est remplacé par une nouvelle agence fédérale, Rossia Segodnia. Sputnik, sa branche internationale, est lancé en octobre 2014, quelques mois après l'annexion de la Crimée. Le journaliste Dmitri Kisseliov, qualifié pour l'occasion de « propagandiste en chef » par *The Economist*, est placé à la tête de l'agence, à l'initiative de Sergueï Ivanov, alors chef de l'Administration présidentielle. Gromov et Lessine obtiennent le poste de rédactrice en chef de Rossia Segodnia pour Simonian, leur protégée. Si son rôle y est moins déterminant que chez RT, Simonian n'en est pas moins devenue, près de quinze ans après sa première nomination, la figure de proue de l'offensive médiatique de la Russie dans l'espace informationnel global.

RT et Rossia Segodnia/Sputnik sont aujourd'hui deux réseaux d'information multilingues et multimédias, dotés respectivement de 2 500 et 2 300 salariés, répartis entre leurs sièges moscovites et plusieurs dizaines de bureaux à l'étranger. RT et Rossia Segodnia ont obtenu du budget fédéral près de 380 millions d'euros en 2019, soit près de 40 % des subventions accordées par l'État aux médias publics (un tiers en 2018). En quinze ans, RT s'est hissé dans le groupe restreint des grandes chaînes de télévision

internationales : son réseau compte en 2019 six chaînes d'information en continu (RT International, RT Arabic, RT en Español, RT America, RT UK et RT France) et une chaîne documentaire (RTD). Elles drainent plus de 100 millions de téléspectateurs chaque semaine, dont 43 millions en Europe. Ses six médias en ligne ont attiré en moyenne, au premier trimestre 2018, 46 millions de visiteurs uniques par mois (SimilarWeb). Sputnik comprend trente et un sites dans des langues étrangères, dont la moitié est destinée à des audiences de l'espace post-soviétique. Hors de cette zone, cinq sites concentrent plus de la moitié des 26 millions de visiteurs uniques de Sputnik ; il s'agit, dans l'ordre décroissant, de Sputnik Türkiye (4,6 millions), de Sputnik Arabic (3,3 millions), de Sputnik France (2,4 millions), de Sputnik Mundo, le site hispanophone (2,2 millions) et de Sputnik Brasil (2,1 millions). À titre de comparaison, les sites de RT, et dans une moindre mesure de Sputnik, sont particulièrement compétitifs dans le trafic Internet mondial, par rapport aux sites des autres médias publics internationaux (tableau n° 2). Sur les deux périodes choisies, RT et Sputnik occupent les deuxième et troisième places, derrière la branche internationale de la BBC.

Tableau 2. – Classement estimé des sites des médias d'audiovisuel public internationaux dans le trafic Internet mondial (source : Alexa)

Médias internationaux (*nom de domaine, NDD*)	**Classement du NDD dans le trafic Web mondial**	
	03/12/2016-03/01/2017	*05/02/2019-05/03/2019*
BBC World (bbc.com)	92e	91e
RT (rt.com)	***276*** **e**	***269*** **e**
Sputnik (sputniknews.com)	***817*** **e**	***594*** **e**
Deutsche Welle (dw.com)	1217e	1247e
Al Jazeera English (aljazeera.com)	2074e	3545e
Radio France Internationale (rfi.fr)	2140e	2233e
Voice of America (voanews.com)	2441e	3026e
France 24 (france24.com)	3956e	4760e
CGTN (cgtn.com)	n/a	15538e
Radio Free Europe/Radio Liberty (rferl.org)	n/a	28145e

Les stratégies de référencement agressives pratiquées par ces deux médias, notamment par un recours décomplexé au *clickbait* (ou « piège à clics », une tactique visant à attirer l'utilisateur sur un contenu, en l'appâtant par un titre racoleur ou provocateur), leur donnent une visibilité accrue sur les principaux moteurs de recherche. Mais c'est surtout sur les réseaux sociaux, où RT et Sputnik ont développé un écosystème complexe de plusieurs dizaines de comptes et où ils servent de ressource à de nombreux acteurs engagés dans la « réinformation » de l'opinion[23], que leurs contenus bénéficient du plus grand potentiel de diffusion.

Les médias russes internationaux cherchent, en effet, à relativiser le rôle et la puissance des pays occidentaux plutôt qu'à améliorer la réputation de la Russie à l'étranger[24]. Le moyen privilégié pour accroître l'influence du pays ne consiste donc pas à renforcer son attractivité, mais à dénigrer son adversaire désigné. Adoptée par RT à partir de la guerre russo-géorgienne

de 2008 et renforcée depuis la crise ukrainienne, cette orientation négative, caractéristique du *soft power* russe, est pleinement assumée par Simonian : « Maintenant, nous ne nous battons plus contre personne. Mais en 2008, nous avons combattu. Le ministère de la Défense s'est battu contre la Géorgie, mais c'est nous qui avons mené une guerre de l'information avec l'ensemble du monde occidental[25]. »

Bien que déclinée en fonction des audiences ciblées, avec des accents relativistes et sarcastiques, la ligne éditoriale alternative de RT reflète un ensemble de positions idéologiques et de représentations du monde manifestement compatible avec l'agenda de politique étrangère du Kremlin : elle affiche un soutien aux forces politiques souverainistes en Europe, souligne l'incapacité des régimes démocratiques libéraux à régler leurs conflits sociaux de manière pacifiée, critique l'interventionnisme et les « prétentions néo-impérialistes » des États-Unis, présente l'Ukraine comme un État dysfonctionnel, défend l'action extérieure de la Russie, notamment en Syrie, etc. Le caractère propagandiste de RT et de Sputnik est sans doute le plus perceptible dans la manière dont ils couvrent les crises impliquant la Russie, comme la guerre du Donbass ou l'affaire Skripal : les chroniqueurs diffusent les éléments de langage du discours officiel et tournent en ridicule les critiques dont Moscou fait l'objet[26]. Enfin, si les modes de communication ont manifestement évolué depuis, il est frappant de constater, dans certains contenus propagés afin de dénigrer une cible donnée, une continuité de nature thématique avec la propagande soviétique, celle de Radio Moscou notamment, dirigée contre « l'ennemi principal » occidental[27].

La manipulation de l'information à des fins de subversion politique

Les manipulations de l'information à des fins de subversion et de déstabilisation se sont également multipliées ces dernières années. Partant du principe que les guerres ne sont plus déclarées et que la Russie subit une guerre de l'information, les plus hauts représentants de l'armée et des services de sécurité n'hésitent pas à recourir à ce que les services secrets soviétiques appelaient des « mesures actives » [активные мероприятия] du KGB pendant la guerre froide. Recensées dans les travaux de Christopher Andrew et Vassili Mitrokhine, à partir des archives sorties par ce dernier, celles-ci s'apparentaient à des « opérations d'influence » clandestines, telles que la manipulation de journalistes, la diffusion de fausses rumeurs, la fabrication de faux, de contrefaçons et de *kompromat*, et le recours à des agents d'influence ; elles étaient destinées à induire l'ennemi en erreur et à discréditer les adversaires de l'Union soviétique auprès de l'opinion internationale[28].

Les efforts de désinformation visent les sociétés et les systèmes politiques de pays considérés comme adverses. Ils se concentrent sur les réseaux sociaux et dans le domaine cyber et ont donné lieu à l'émergence de nouveaux acteurs et de nouvelles pratiques. L'Agence de recherche Internet, connue sous l'acronyme anglais IRA, est décrite comme une « usine à trolls ». Créée, selon toute vraisemblance en 2013, et installée à Saint-Pétersbourg, elle est financée par l'homme d'affaires Evgueni Prigojine, qui possède la société militaire privée russe Wagner. Le procureur spécial Robert Mueller, chargé d'enquêter sur les ingérences russes dans la campagne présidentielle américaine, a mis en cause l'IRA dans son rapport[29]. Il a notamment dénoncé ses campagnes de *trolling*, ce phénomène visant à « influencer les valeurs, croyances, perceptions […] et comportements de communautés ciblées » sur les réseaux sociaux, en recourant à la parodie, à la satire, voire au harcèlement des usagers[30]. Selon ses accusateurs, l'IRA aurait propagé entre 2015 et 2017 aux États-Unis, sur Facebook, Instagram et Twitter, des contenus favorables au candidat Donald

Trump, nuisibles à son opposante Hillary Clinton ou destinés à polariser la société américaine en attisant les tensions intercommunautaires, sans que l'on puisse toutefois mesurer leur efficacité et leur incidence sur le résultat des élections[31]. Si l'IRA a été amplement médiatisé, l'impact réel de ces campagnes de désinformation, du reste principalement composées de contenus anglophones, reste largement méconnu.

Un autre phénomène, qui peut s'articuler au précédent, consiste à procéder à des cyberattaques, soit pour mettre hors service les systèmes informatiques de ses adversaires, soit pour soustraire des données confidentielles et les dévoiler au public, par exemple lors d'un processus électoral, de façon à semer la confusion et influencer le résultat. La Russie est à ce titre considérée comme une puissance – et une menace – cybernétique de premier plan. Si la question de l'attribution de ces attaques reste hautement problématique, Moscou est souvent considéré comme responsable de la première cyberattaque jamais lancée contre un État tiers, l'Estonie, en 2007[32]. Des groupes de hackers russes ont piraté des serveurs du Comité national du Parti démocrate (DNC) en juillet 2016 – une opération d'hameçonnage pourtant peu sophistiquée, par laquelle le groupe de hackers APT28 (ou *Fancy Bear*) aurait récupéré des e-mails du DNC, qu'ils ont transmis à l'organisation WikiLeaks pour porter atteinte à la candidate démocrate. De même, à la veille du second tour de l'élection présidentielle française de 2017, des rumeurs sur le candidat Emmanuel Macron et des e-mails volés (les « Macron Leaks ») ont été opportunément diffusés, éveillant les soupçons d'une opération menée par des hackers russes[33].

Le contrôle de l'information dans les opérations armées

Les technologies de l'information ont également modifié l'art de la guerre. La révolution numérique a permis de réduire l'espace-temps sur le champ de bataille en améliorant la connaissance de l'environnement de combat, la coordination des forces armées déployées et la communication entre les différents niveaux de décision. Mais elle a aussi transformé la communication de guerre : il est désormais possible de médiatiser en temps réel, images à l'appui, une opération militaire, une défaite ou une victoire et, ce faisant, d'exercer une action directe sur l'arrière et l'opinion publique de l'adversaire. Dans son article de 2013, le chef d'état-major Guerassimov accordait une grande importance à ces deux particularités des guerres contemporaines :

> Le rôle des corps de troupes mobiles, de différents types, agissant dans un même espace d'information et de renseignement, s'accroît en raison de l'utilisation des nouvelles potentialités des systèmes de commandement et d'approvisionnement. Les actions militaires deviennent plus dynamiques, plus actives, et donnent plus de résultats. Les pauses tactiques et opératives dont l'adversaire pourrait tirer profit disparaissent. Les nouvelles technologies de l'information ont permis de réduire de façon significative la rupture entre les troupes et les organes de commandement en termes d'espace, de temps et d'information. […]
> L'influence à distance, sans contact, sur l'adversaire devient le principal moyen d'atteindre ses objectifs de combat et d'opération. La défaite de ses entités s'effectue dans toute la profondeur du territoire. Les distinctions s'effacent entre les niveaux stratégiques, opératifs et tactiques, et entre les actions offensives et défensives. Le recours à des armements de haute précision se généralise. Des armes fondées sur de nouveaux principes physiques et des systèmes robotisés sont introduits activement dans la chose militaire [34].

Si l’apparition du numérique et la robotisation des armements améliorent l’efficacité opérationnelle sur le champ de bataille, elles constituent en même temps une vulnérabilité nouvelle. Pour affirmer sa suprématie dans le domaine informationnel, l’armée russe a développé un ensemble d’outils et de techniques lui permettant de mener des actions technico-informationnelles et psychologico-informationnelles. Elle concentre actuellement ses efforts dans trois directions : le perfectionnement de la guerre électronique, l’extension des opérations psychologiques et le développement d’armes de destruction des infrastructures matérielles.

Sur le champ de bataille, la guerre de l’information s’est d’abord matérialisée par la guerre électronique qui suppose le brouillage des communications adverses. Les interventions dans le champ électromagnétique se sont perfectionnées ces dernières années ; elles permettent désormais de saper la supériorité informationnelle de l’adversaire en perturbant ses moyens de commandement et de navigation et en neutralisant ses outils d’information et de communication, notamment ses capacités de renseignement, de reconnaissance et de ciblage. En matière de guerre électronique, l’armée russe possède des capacités sophistiquées qui se déclinent sur l’ensemble du spectre capacitaire et qui, de surcroît, associent des opérations de guerre psychologique.

Au début de la guerre en Ukraine, l’armée russe a ainsi utilisé « le brouillage en vue de la protection de force ou le leurrage de l’adversaire », en combinant ces actions à des opérations de démoralisation. Comme l’explique le colonel Patrick Justel, il s’agissait de « leurrer les missiles adverses ou de déclencher l’explosion prématurée des munitions » et « d’attaquer les moyens de communication, de localisation (GPS) et de renseignement ennemis (drones) afin de rendre ce dernier aveugle ». Mais il s’agissait aussi de porter atteinte au moral des soldats et de les géolocaliser

en annonçant par SMS leur mort à leurs proches qui les exposaient en tentant de les joindre[35].

Des appareils militaires sont élaborés pour dominer le spectre électromagnétique et accroître les capacités de brouillage sur terre, sur mer et dans les airs. Cependant, l'objectif de la guerre électronique n'est plus seulement de contrôler les flux d'information dans une zone de conflit, mais de cibler des combattants ennemis et d'exercer sur eux une pression psychologique. Embarqué sur un drone, le système Leer-3 renforce les capacités aéroportées de brouillage offensif de l'armée russe ; il permet également de pirater plusieurs milliers de téléphones portables ennemis en même temps, de leur envoyer des SMS, des images et des vidéos, tout en bloquant leurs communications et en préservant celles de son camp[36].

En parallèle des moyens classiques de guerre électronique qu'elle continue de perfectionner, l'armée russe se dote de structures chargées d'exercer une action psychologique. En 2017, des « forces d'opérations d'information » ont été créées afin de mener une « propagande intelligente, élaborée et efficace », d'après les déclarations du ministre de la Défense Sergueï Choïgou. Ces unités qui appartiennent aux forces armées conventionnelles procèdent à des opérations d'influence au niveau tactique et opératif en agissant dans toute la profondeur du territoire : elles élaborent des opérations psychologiques visant à la fois des combattants sur le terrain d'opération et des civils à l'arrière.

Les autorités militaires russes s'intéressent de plus en plus aux potentialités offertes par l'analyse de *big data*. L'intelligence artificielle pourrait permettre dans le futur de créer des machines qui apprendraient à façonner l'information en fonction d'audiences cibles et qui pourraient ainsi conduire des opérations d'information sur mesure à grande échelle[37]. Ces nouvelles technologies de l'information ouvrent de nouveaux champs d'applications pour certains concepts-clés de l'art opératif soviétique, tels que l'action en profondeur, qui vise non pas à détruire une cible matérielle

ou l'intégralité d'un système ennemi (ce qui est souvent impossible), mais à empêcher son fonctionnement en détruisant sa cohésion.

En dernier lieu, l'armée russe renforce ses moyens de coercition et de destruction sur des infrastructures civiles et militaires. Elle peut déjà lancer des attaques cyber en appui d'une opération militaire afin de détruire les moyens de communication de l'adversaire au niveau stratégique et tactique, et ainsi paralyser ses capacités de réaction, comme lors de la guerre russo-géorgienne d'août 2008[38]. Elle cherche maintenant à développer des armements capables d'anéantir les moyens de communication adverses. Des armes sont élaborées dans le but de détruire les couches matérielles des télécommunications et du cyberespace : le système Nudol permet d'abattre des satellites en orbite basse ; des sous-marins espions pourraient servir à couper des câbles sous-marins, par lequel transite le trafic des données.

*

L'espace informationnel est perçu en Russie comme le théâtre d'un jeu à somme nulle. Les autorités russes l'appréhendent comme un environnement compétitif au sein duquel des puissances rivalisent pour influencer des publics cibles à l'étranger. Comme au temps de la guerre froide, l'information sert moins à accroître la réputation de la Russie qu'à discréditer « l'Occident libéral » comme référent politique et normatif. Les dirigeants russes considèrent aussi l'espace informationnel comme un véritable terrain de conflictualité. Dans un conflit armé, l'objectif est de prendre le dessus sur le terrain d'opération, mais aussi de préserver ses arrières et de priver l'ennemi de ses ressources. De même, la protection de la « souveraineté informationnelle » ne se résume pas à lutter contre des manipulations étrangères supposées ou des attaques cybernétiques potentielles, même si elle s'accompagne d'une limitation grandissante des libertés publiques et individuelles et d'un contrôle renforcé des acteurs du Web. La « sécurité informationnelle » du pays requiert, selon la conception

qui prévaut dans des cercles du pouvoir russe, de conduire des actions offensives et des opérations subversives à l'étranger afin d'endommager et de pénétrer l'espace informationnel de l'adversaire pour en tirer un bénéfice, qu'il soit tactique ou stratégique. Plus que les moyens déployés, c'est cette conception totale et instrumentale de l'information qui rappelle le plus la période soviétique.

Pour aller plus loin

AUDINET Maxime, « Diplomaties publiques concurrentielles dans la crise ukrainienne : le cas de RT et Ukraine Today », *Revue d'études comparatives Est-Ouest*, 2018, vol. 2, n° 2, p. 171-204.

DAUCÉ Françoise, ERMOSHINA Ksenia, LOVELUCK Benjamin et MUSIANI Francesca, « Souveraineté numérique : l'Internet russe peut-il se couper du reste du monde ? », *The Conversation*, 18 mars 2019.

KISELEVA Yulia, « Russia's soft power discourse : Identity, status and the attraction of power », *Politics*, 2015, vol. 35, n° 3-4, numéro spécial intitulé « The soft power of hard states, p. 316-329 ».

LIMONIER Kevin, AUDINET Maxime, « La stratégie informationnelle et numérique de la Russie en Europe », *Hérodote*, 2017, n° 164, p. 123-144.

MARANGÉ Céline, *Les Stratégies et les Pratiques d'influence de la Russie*, Paris, IRSEM, *Études*, n° 49, 2017, 55 p.

POPESCU Nicu, SECRIERU Stanislav (dir.), « Hacks, leaks and disruptions. Russian cyber strategies », *Chaillot Paper*, octobre 2018, n° 148, 129 p.

SZOSTEK Joanna, « Nothing is true ? The credibility of news and conflicting narratives during "information war" in Ukraine », *The International Journal of Press/Politics*, 2018, vol. 23, n° 1, p. 116-135.

YABLOKOV Ilya, « Conspiracy theories as a Russian public diplomacy tool : The case of Russia Today », *Politics*, 2015, vol. 35, n° 3, p. 301-315.

RESISTIC, « Les résistants du Net. Critique et évasion face à la coercition numérique en Russie », projet de recherche réunissant cinq centres de recherche partenaires. Voir https://www.resistic.org.

CHAPITRE 5

La Chine : une modernisation des pratiques de guerre de l’information

Valérie Niquet

Le concept de guerre de l’information est au cœur de la pensée stratégique chinoise et s’exprime sous plusieurs formes qui vont de la propagande aux derniers développements de la guerre cybernétique et de l’intelligence artificielle. À l’époque contemporaine, la guerre de l’information, en raison de la nature du régime politique léniniste de la République populaire de Chine (RPC), s’adresse autant à la population chinoise qu’à l’extérieur, tout en préservant le principe 内外别 (l’intérieur et l’extérieur sont différents) de différenciation de l’information. Cette centralité s’appuie sur un corpus d’écrits stratégiques au premier rang desquels figure *L’Art de la guerre* de Sun Zi et qui, dès le IVe siècle avant notre ère, ont placé l’économie et l’utilisation des moyens détournés au centre de leur enseignement[1]. Cette tradition a été renforcée par l’apport léniniste et redécouvert à une période plus récente par les penseurs de la guerre asymétrique qui permet d’inverser les rapports de force[2].

À l’époque contemporaine, avec la montée en puissance des capacités technologiques, la dimension strictement militaire de la guerre de

l’information a acquis en Chine une importance considérable, qui prend en compte les évolutions conceptuelles de la pensée stratégique américaine, nouvelle « menace principale » contre laquelle l’APL (Armée populaire de libération) doit se préparer en ultime ressort. Parallèlement, la dimension plus classique de guerre de propagande et d’influence n’a pas disparu, renforcée au contraire par les nouveaux moyens de contrôle et de communication maîtrisés par le régime chinois.

L’appréhension des guerres de l’information en Chine est donc particulièrement complexe, avec des éléments civils et militaires, technologiques et idéologiques, anciens et très contemporains sans qu’une véritable rupture se soit produite dans la réflexion stratégique.

Les fondements théoriques de la guerre de l’information en Chine

La guerre de l’information en Chine se nourrit de deux courants compatibles qui sont la pensée stratégique classique et l’inspiration léniniste. Ces deux courants sont au cœur de la pensée stratégique de Mao Zedong, théorisée avant la prise du pouvoir du parti communiste en 1949. Ces trois héritages sont adaptés à la situation d’asymétrie – caractérisée par un rapport de forces qui lui est défavorable – dans laquelle se trouve la RPC face à la puissance américaine.

Ruse et stratagème : l’héritage classique

La prise en compte du coût de la guerre et des combats, le refus du beau geste ou de l’acte héroïque, la place prépondérante accordée au « civil » sur le « militaire » à l’époque impériale constituent les fondements conceptuels

de l'importance accordée à la guerre de l'information en Chine[3]. La « guerre », à l'époque impériale, est assimilée au maintien de « l'ordre » et de l'harmonie, dans un continuum qui s'étend du cœur aux marges de l'Empire. Il s'agit de « séduire » et de « convaincre » l'adversaire, de le « siniser », toute invasion étrangère, même celles qui ont entraîné un effondrement dynastique n'aboutissent en fait qu'à la victoire de la Culture (文) sur la barbarie. Cela a notamment été le cas pour la dynastie « chinoise » des Qing, peuple nomade mandchou qui, de 1644 à 1911, a gouverné la Chine en reprenant tous les codes de sa culture classique, dont le confucianisme. Plus que de conquêtes territoriales – même si celles-ci ont existé – il s'agit d'un combat idéologique visant à imposer la reconnaissance universelle de la centralité de l'Empereur de Chine. Perdre la guerre, c'était aussi perdre le « mandat du Ciel » et la justification idéologique de la survie d'une dynastie, remplacée par une autre investie d'une légitimité renouvelée.

L'Art de la guerre de Sun Zi, composé vraisemblablement autour du IIIe siècle avant notre ère, alors que les combats entre royaumes faisaient rage, fonde les principes de cette guerre de l'information à la chinoise[4]. Pour Sun Zi, la guerre est un acte total, qui prend en compte le coût économique, humain, mais aussi politique et idéologique. Dès le premier chapitre, *L'Art de la guerre* souligne la nécessité de « calculs » et affirme que « la guerre, c'est l'art de duper ». Pour Sun Zi, comme pour l'essentiel des textes ultérieurs qui composent le corpus des classiques de la stratégie chinoise, la ruse, les stratagèmes, la manipulation, sont au cœur de l'art de la guerre[5]. Selon Sun Zi, « celui qui est incapable doit faire croire qu'il est capable, celui qui est prêt au combat doit faire croire qu'il ne l'est pas, celui qui est fort doit faire croire qu'il est faible, celui qui est faible doit faire croire qu'il est fort[6]… ». À l'époque de Sun Zi, comme au XXIe siècle, il s'agit donc de « brouiller » la perception de l'ennemi.

L’objectif est de « soumettre l’ennemi sans combattre », de « remporter la victoire sur un ennemi battu d’avance ». Le coût, économique, social et donc politique de la guerre est bien trop important pour un aventurisme inutile. En revanche, il ne s’agit pas de s’interdire les bénéfices d’une guerre par d’autres moyens – stratégie d’influence, désinformation, guerre psychologique – qui ne sont pas strictement « militaires ».

La supériorité dépend donc de l’information, et le dernier chapitre, consacré aux espions, le confirme. Pour Sun Zi, ce sont les « espions », et non la « divination » qui permettent de maîtriser l’information. Les agents d’influence, les agents « de l’intérieur », placés auprès des princes ennemis, les agents retournés, les agents sacrifiés et ceux qui doivent vivre, pour rapporter des renseignements essentiels sont tous nécessaires à la manipulation de l’ennemi[7]. Cette pensée classique irrigue toute la pensée stratégique chinoise. Elle est particulièrement adaptée à l’état d’asymétrie des forces chinoises – en dépit des progrès considérables méthodiquement accomplis depuis le début des années 1990 – face aux États-Unis, seule puissance capable de limiter la marge de manœuvre de la République populaire de Chine en Asie.

Manipulation et propagande : l’apport lénino-maoïste

Ce même souci d’économie et de pragmatisme dans une situation d’asymétrie a été renforcé par l’apport lénino-maoïste dans la période de conquête du pouvoir avant 1949. À ce souci « d’économie » et de contournement de l’adversaire, s’est ajoutée une puissante dimension de propagande (*agit-prop*) qui a fortement contribué à la victoire du Parti communiste chinois sur son adversaire du Kuomintang à la tête de la République de Chine[8].

Mao Zedong a été fortement inspiré, en dépit de ses dénégations ultérieures, par la culture stratégique chinoise classique et par le léninisme.

Le calcul des coûts d'une opération en fonction de l'objectif ultime, la transformation du rapport du faible au fort, la propagande et la manipulation sont au cœur de la pensée maoïste de prise et de contrôle du pouvoir. Pour Mao, la supériorité idéologique l'emporte sur la supériorité matérielle[9]. Il est nécessaire de connaître les forces et les faiblesses de l'adversaire pour mieux les exploiter.

La propagande joue un rôle essentiel. Il s'agit pour Mao de « gagner la sympathie » à l'intérieur et à l'extérieur par tous les moyens de la guerre de l'information. La mobilisation politique et le contrôle idéologique interne sont l'un de ces moyens. Les « Discussions sur la littérature et l'art » prononcées à Yan'an par Mao en 1942 fonderont tout le travail de contrôle idéologique avant et après la conquête du pouvoir[10]. Il s'agit d'établir fermement la direction du parti sur le travail de propagande, et ce principe est toujours celui qui préside aujourd'hui au travail idéologique du Parti communiste chinois.

La projection d'une image positive vers l'extérieur est tout aussi importante pour « briser les alliances de l'ennemi » comme l'écrivait Sun Zi. À Yan'an, où les forces communistes s'étaient réfugiées après la retraite stratégique de la Longue Marche (1934-1935), la « propagande extérieure » prend une importance considérable. Il s'agit de séduire les États-Unis, alliés du Kuomintang au pouvoir, en construisant l'image d'un parti honnête, non corrompu et jouant un rôle majeur dans la guerre contre le Japon. Des journalistes américains reçus à Yan'an, tels Edgar Snow, ou fréquentant les troupes communistes, comme Agnes Smedley, ont été séduits et ont contribué à répandre cette image[11]. Dans le même temps, l'URSS contribuait aussi à étayer cette image, favorable, à partir de leur entrée en guerre, au rapprochement entre le Parti communiste chinois et les États-Unis[12].

À la veille d'accueillir des correspondants de journaux américains à Yan'an en 1944, le département de la propagande du parti communiste

reçoit la mission de préparer des documents sur le caractère démocratique du parti et sur le sauvetage de pilotes américains par les forces communistes. L'ambassade des États-Unis à Chongqing, où s'est replié le gouvernement nationaliste, est également nourrie de chiffres qui tendent à prouver que « 58 % » des forces japonaises en Asie sont immobilisées grâce aux unités de l'Armée rouge du Parti communiste chinois[13].

Cette stratégie de guerre de l'information en direction des États-Unis pour affaiblir leur soutien au Kuomintang rencontre un véritable succès puisque les conseillers américains de Chiang Kaï-shek, alors à la tête de la République de Chine, vantent « l'honnêteté des communistes » face à la « corruption des nationalistes ». Pour l'ambassadeur des États-Unis en Chine, John Stuart Service, « il ne fait aucun doute que les armées communistes sont des alliés utiles[14] ». Après 1945, alors que la Chine replongeait dans la guerre civile, les États-Unis ont fait pression pour que le Kuomintang accepte de négocier avec le parti communiste, et la République de Chine ne reçoit aucun soutien pour reprendre possession de la Mandchourie, qui devient, avec l'appui de l'URSS, la base industrielle et de conquête du parti communiste.

Le contrôle de l'information à l'époque contemporaine : propagande et contre-propagande

On retrouve l'ensemble des éléments précédents à l'époque contemporaine, avec une remontée en puissance de la dimension idéologique depuis le début des années 2010 et l'arrivée au pouvoir de Xi Jinping en 2012. À partir de 1979, avec la mise en œuvre d'une politique pragmatique d'ouverture et de réformes économiques, le contrôle politique

et le poids de la propagande sur la population se sont, dans un premier temps, considérablement réduits. Les années 1980, jusqu'à la répression de la place Tian an men en 1989 et à la chute de l'URSS, ont été des années de grande libéralisation idéologique. À partir des années 1990, le contrôle s'est à nouveau renforcé, avec la généralisation de « l'éducation patriotique » et la montée du nationalisme comme facteur de légitimité. Mais dans le même temps, sur la scène internationale, la Chine privilégie les concepts « d'émergence pacifique » (和平崛起) et « d'harmonie » (和谐), fondés sur la patience stratégique et la modestie apparente, favorables au renforcement discret des positions chinoises sur la scène internationale [15].

Les organes du parti en charge de la propagande interne

La propagande et le contrôle de l'information en interne ne sont pas nouveaux en Chine, et, suivant le modèle du Kominterm, remontent à la création du Parti communiste chinois en 1921. Par ailleurs, dès les premières bases « rouges » à la fin des années 1930 et après 1949, la surveillance idéologique de la population, par l'intermédiaire des comités de quartiers omniprésents et du livret individuel (档案), qui suit un individu depuis ses premières années scolaires, n'a pas connu d'interruption, allégée toutefois après 1979 jusqu'aux années 2000. L'arrivée au pouvoir de Xi Jinping a renforcé le contrôle idéologique.

Désormais de nouveaux instruments ont été mis au service de cette surveillance idéologique. Les ressources de l'intelligence artificielle, le traçage électronique, encore renforcé depuis l'épidémie de Covid-19 au nom de la santé publique, et le système de « points » (système de confiance sociale 社会信用体系), mis en place en 2014, ouvrent ou ferment des opportunités [16]. Des applications permettent également de distribuer des « bons » ou des « mauvais » points idéologiques selon le niveau de

connaissance de la « Pensée Xi Jinping ». L'aspect « ludique » et l'intéressement financier avec un système de bons d'achat sont venus renforcer cette stratégie de contrôle idéologique.

Au sommet du parti – et de l'État – le département de la propagande du Comité central du parti communiste (宣传部) joue un rôle essentiel avec son pendant étatique, le ministère de l'Information. Le département est en charge de tout le travail idéologique et de la censure des médias, encore renforcée depuis l'arrivée au pouvoir de Xi Jinping, par l'intermédiaire de l'administration générale de la presse et des publications. Le département contrôle également la radio, la télévision et la production cinématographique.

Le rôle d'Internet : ouverture initiale et adaptation de la censure

Les années 1990 ont coïncidé avec l'arrivée d'Internet en Chine, avec une progression d'abord lente puis exponentielle à partir de 1994, date du premier raccordement de la Chine aux réseaux. La multiplication des cybercafés, puis des ordinateurs et surtout des téléphones portables, a véritablement marqué l'entrée de la Chine dans un monde de liberté d'accès à des informations longtemps contrôlées. En 1996, le Conseil des affaires de l'État publiait toutefois une première directive sur la régulation d'Internet et des réseaux sociaux, prévoyant notamment un contrôle physique des voies d'entrée d'Internet en Chine. La mobilisation massive de militants du mouvement Falungong pour une manifestation organisée au cœur de Pékin en 1999 a suscité une crainte majeure du pouvoir et les contrôles se sont renforcés. Toutefois, les sites étrangers sont restés largement accessibles, facilitant les échanges et l'information de la population urbaine.

À partir du début des années 2000, un système de plus en plus étanche de pare-feu et de contrôle idéologique a été mis en place à l'échelle de la Chine, s'appuyant sur le concept de « souveraineté de l'espace cyber ». Selon ce concept, chaque pays doit pouvoir choisir son propre modèle de régulation et d'ouverture[17]. Sur la scène internationale, la Chine, avec la Russie, a également tenté d'imposer au nom de la sécurité son propre système de normes fondé sur le découplage de l'Internet global[18]. En 2015, la Chine a également développé le concept de « Routes de la soie numériques », permettant de développer la connectivité mais aussi d'avoir accès aux informations au service des intérêts de la RPC[19].

Fang Bingxing, président de l'Université des postes et télécommunications de Pékin de 2007 à 2013, a mis en place en 2001 le Computer Network Emergency Response Technical Team of China (CNCERT) sous la direction du ministère de l'Industrie et des Technologies de l'information. Dans un premier temps, l'idée était aussi de laisser s'exprimer certaines critiques afin d'améliorer l'information des autorités, quitte à réprimer a posteriori. Un tournant s'opère à partir de l'arrivée au pouvoir de Xi Jinping à la tête du parti en 2012 puis de l'État au mois de mars 2013. Cette même année, Xi Jinping a prononcé un discours décrivant Internet comme « un nouveau champ de bataille dans la guerre pour l'opinion publique, contre les forces occidentales antichinoises[20] ».

En 2014, la Cyberspace Administration of China (CAC) (互联网信息办公室) a également été mise en place, sous l'autorité directe du parti communiste et du président Xi Jinping, qui dirige la commission des affaires cybernétiques du Comité central (中央网络安全和信息化委员会) instaurée en 2013. La mission de cette administration, au service de la propagande intérieure et extérieure du parti communiste, est de promouvoir les éléments positifs et de supprimer les éléments négatifs, nuisibles à la stabilité sociale et souvent perçus comme une offensive externe destinée à aboutir – comme avec les Printemps arabes – à un changement de régime[21].

Le contrôle a donc été renforcé, avec la mise en place d'un système de filtres, de suppression des adresses IP, d'obligation d'identification, d'attaques de masse contre des sites considérés comme « hostiles » fondées sur l'utilisation de dizaines de milliers de « soldats du Net », rémunérés pour chaque post. Le système est par ailleurs mobile et adaptable, suivant l'évolution des technologies. Les VPN, qui étaient l'un des principaux moyens de contournement, sont interdits, les « bots » ont remplacé en partie les « soldats du Net ».

En 2017, la *Cyber Security Law* renforce l'ensemble des contrôles, au nom de la lutte contre les crimes cybernétiques. Elle renforce notamment le contrôle d'utilisation des VPN. Toutes les entreprises, chinoises ou étrangères, doivent conserver leurs données et en permettre l'accès aux autorités. Par ailleurs, les compagnies chinoises doivent exercer une forme d'autocensure en renforçant leurs propres équipes de contrôle. C'est le cas notamment de TikTok qui a mis en place une équipe de plus de 10 000 contrôleurs des contenus qui transitent par sa plateforme [22].

Coïncidant avec la mise en place du pare-feu idéologique (*Great Firewall*), les navigateurs, sites et applications étrangers ont progressivement été interdits, Google, WhatsApp, le New York Times, le Wall Street Journal, Bloomberg parmi les plus importants. Ces sites ont été remplacés par des clones chinois, Baidu, Weibo, Wechat, Tencent, mais aussi par Alibaba (clone d'Amazon) qui ont vu leur développement croître d'une manière exponentielle en l'absence de concurrence internationale.

Toutefois, en dépit de ces moyens de contrôle considérables et de contre-propagande adaptés aux nouvelles conditions technologiques, la Chine compte désormais plus de 800 millions d'utilisateurs d'Internet. En période de crise majeure, comme l'a démontré la crise du Covid-19 en 2020, le contrôle absolu de l'information devient très difficile et Internet continue de jouer un rôle important d'expression des frustrations et des mécontentements. Internet est également pleinement intégré à la « guerre de

propagande » à vocation externe que mène avec une activité renforcée le régime chinois.

Le rôle de la propagande extérieure dans la guerre de l'information

Cette dimension de la guerre de l'information est essentielle pour le régime chinois. Au milieu des années 1990, les stratèges chinois rappellent cette dimension de propagande et de « guerre psychologique » de la guerre de l'information qui permet de manipuler l'ennemi et d'en obtenir des avantages, jusqu'à la victoire qui, dans le domaine civil, correspond à la transformation du système mondial au service des intérêts de Pékin[23].

Des objectifs en évolution

La propagande extérieure a toujours pour objectif de renforcer l'image de la Chine à l'extérieur, de gagner des soutiens et d'augmenter la marge de manœuvre de Pékin. En diffusant l'image d'une puissance dont l'émergence est inéluctable, les appareils de propagande contribuent aussi à étayer l'attractivité économique du pays qui est indispensable à la poursuite des investissements étrangers et des transferts de technologie dont la Chine a besoin.

Plusieurs thématiques se sont succédé dans le discours de propagande extérieur à partir des années 1990. Dans un premier temps, le concept « d'émergence pacifique » (和平崛起) s'est imposé. Destiné à rassurer les partenaires de Pékin en encourageant les stratégies « d'engagement » et à obtenir notamment l'intégration de la Chine à l'OMC (Organisation

mondiale du commerce), il permet à partir de 2001 le développement fulgurant de la croissance chinoise.

Depuis, avec l'arrivée au pouvoir de Xi Jinping en 2012, le discours s'est durci et des thématiques comme celle de la « place centrale sur la scène internationale » (世界舞台中) sont mises en avant, signant l'émergence de la Chine au premier rang des puissances. La propagande extérieure a également permis à la Chine de renforcer son poids au sein des organisations internationales dépendantes ou non de l'ONU, au service des intérêts de Pékin[24]. La propagande extérieure permet de mobiliser les pays du Sud contre l'Occident en rappelant à la fois le « passé commun » anticolonial et anti-impérialiste et le poids économique et financier de la Chine contemporaine.

Des instruments intégrés et diversifiés

La République populaire de Chine mobilise des moyens diversifiés au service d'une propagande extérieure qui demeure souvent peu efficace en raison de la nécessité, pour sa mise en œuvre, de ne pas s'éloigner de la « ligne officielle », même si celle-ci, comme l'a démontré la crise du Covid-19, s'avère très peu adaptée aux objectifs et au public visés et entraîne des réactions hostiles.

Au sommet des organes de propagande extérieure, qui dépendent de la commission des affaires extérieures du parti communiste avec à sa tête Xi Jinping, on trouve le Groupe dirigeant pour le travail de propagande et idéologique (中央宣传思想领导组), dont dépendent les organes de propagande extérieure (对外宣传), avec le bureau d'information du conseil de l'État (国务院新闻办公室). Ces organes contrôlent et organisent le travail de propagande extérieure dans toutes ses dimensions. Les organes de l'État et les ministères, dont le ministère des Affaires étrangères qui a un rôle de mise en œuvre à travers notamment le réseau d'ambassades, le

ministère de la Culture, et celui de l'Éducation sont intégrés à ces structures. C'est également le cas de l'agence de presse Xinhua, des grands journaux tels que *Le Quotidien du peuple* (人民日报) ou le *Global Times* (环球时报), particulièrement actif sur Twitter. Enfin, de grandes entreprises comme Alibaba ou Huawei pourraient être mobilisées au service de l'image de la Chine.

Le travail de « front uni » (统战部), qui consiste à mobiliser des classes sociales ou des organisations qui ne sont pas les classes ouvrières ou paysannes et ne sont pas membres du parti communiste pour obtenir leur soutien, remonte aux origines du parti communiste. Ce travail occupe une place particulièrement importante pour mobiliser les communautés chinoises d'outre-mer et les soutiens de Pékin à Hong Kong et à Taïwan. La mobilisation et la surveillance des communautés chinoises – notamment les étudiants – au travers des ambassades, se sont également accrues depuis l'arrivée au pouvoir de Xi Jinping. La Chine tente notamment d'influer sur le programme des universités où d'importantes cohortes d'étudiants chinois sont présentes comme en Australie.

La propagande chinoise a également évolué dans sa forme, si ce n'est dans son contenu, avec l'évolution des technologies. La presse, la radio, la télévision ont vu leurs moyens considérablement renforcés, avec le financement de chaînes de télévision en langue anglaise et française, notamment à destination de l'Afrique, ou l'achat de pages, qui ressemblent à des reportages mais sont en réalité des articles de propagande fournis par les agences de presse officielles chinoises dans des journaux à l'étranger.

Le développement des Instituts Confucius – qui dépendent directement du bureau de la propagande du comité central – lui-même favorisé par un discours mettant en avant la normalisation et l'engagement du régime chinois – participe de la même évolution[25].

À partir de la fin des années 2010, la propagande chinoise – y compris en mobilisant ses représentations à l'étranger et les porte-parole du

ministère des Affaires étrangères – s'est emparée de moyens interdits en Chine même, et plus particulièrement du réseau Twitter. Le ton, encouragé par la direction du parti communiste et Xi Jinping, est beaucoup plus agressif, dénonçant régulièrement les « éléments antichinois » et participant aux opérations de désinformation[26].

La dimension militaire de la guerre de l'information

Dès son arrivée au pouvoir à la tête du parti communiste et de la Commission militaire centrale en 2012, le président Xi Jinping a appelé l'APL à être « prête au combat ». Les campagnes de lutte contre la corruption, initiées par le nouveau président, ont été particulièrement sévères au sein de l'APL et ont permis une reprise en main idéologique. En 2014, Xi Jinping a appelé à « former une nouvelle armée du peuple », rappelant la domination absolue du parti sur l'armée et l'urgence du travail politique dans une situation de grande tension idéologique[27]. La guerre de l'information fait par ailleurs partie de la panoplie légitime de l'APL comme le développaient pour le grand public les auteurs de *La Guerre hors limites*, deux colonels de l'APL, en 1999.

Mais au-delà de cette dimension de guerre idéologique, l'APL a également considérablement développé la dimension technologique de la guerre de l'information, inspirée par les travaux de Andrew Marshall aux États-Unis sur la révolution dans les affaires militaires. En 1991, le choc de la première guerre du Golfe avait fait prendre conscience à la Chine des limites considérables de ses propres capacités. La seconde guerre d'Iraq en 2003 et le renversement de Saddam Hussein ont conforté ce sentiment d'urgence.

Renouvellement conceptuel et mise en œuvre des moyens

Sur le plan conceptuel, de nombreuses publications américaines, traduites en chinois, ont servi de fondement à la réflexion stratégique chinoise sur la guerre de l'information, d'autant qu'elles ont favorisé la redécouverte des classiques de la stratégie chinoise au sein du département d'études stratégiques de l'Académie des sciences militaires.

Le concept de « contrôle de l'information » ou « supériorité » dans le domaine de l'information est devenu central dans la réflexion des stratèges chinois. Amorcée dès 1991, la réflexion se poursuit et, à partir de 2004, la Chine se prépare à « remporter un conflit local dans les conditions de la guerre de l'information[28] ». La priorité est d'élever le niveau technologique de l'APL en poursuivant parallèlement « l'informatisation » et « la mécanisation »[29]. Dans un contexte très asymétrique face aux États-Unis, la guerre de l'information permet au plus faible de l'emporter sur le plus puissant en s'attaquant à ses points forts, qui sont aussi les principaux nœuds de faiblesse de l'adversaire. C'est le cas notamment des réseaux de communication par Internet et de tous les systèmes de contrôle vitaux pour le fonctionnement des grandes entreprises.

La mise en place de moyens détournés, civils ou militaires, permet selon les stratèges chinois, et comme le prônait Sun Zi, de « vaincre sans combattre », sans recours à l'usage de la force face à un ennemi matériellement très supérieur. Dans cette guerre sans limites, la diplomatie, la « guerre légale », la guerre psychologique, l'économie, sont autant de moyens de coercition qui doivent être utilisés pour atteindre l'objectif politique fixé par le parti communiste.

Les objectifs de cette « guerre de l'information » doivent être pour la Chine de se doter des moyens de contrôler l'information, dissimuler ses capacités, au premier rang desquelles les capacités balistiques et nucléaires qui constituent le cœur de la véritable puissance d'interdiction de la Chine,

au moyen de leurres, d'opérations de désinformation, de système permettant d'aveugler les moyens d'observation ennemis, y compris dans l'espace. Au niveau offensif, la Chine doit se doter des moyens de détruire les réseaux de communication de l'ennemi, les systèmes C4I, les centres de contrôle des données, essentiels à la logistique et aux armes de précision de l'ennemi[30]. Les stratèges chinois notent par exemple l'utilisation de virus pour paralyser le système de radar irakien pendant la seconde guerre du Golfe ou les dommages infligés au programme nucléaire iranien[31].

La guerre de l'information permet également de brouiller un peu plus les limites entre guerre et paix, entre victoire et défaite. Par ailleurs, le concept de l'information est étendu à de nouveaux champs de bataille dans l'espace ou dans le cyberespace qui s'ajoutent aux terrains traditionnels[32]. Les capacités de nuisance et d'interdiction de la Chine se développent avec sa montée en puissance technologique globale, notamment dans le domaine cybernétique. Les capacités C4I, point fort des forces américaines et de leurs alliés, dépendent fortement du spatial. Dès le milieu des années 2000, Pékin a inauguré une série d'essais ASAT, dont le premier tir réussi, aboutissant à la destruction d'un satellite météorologique en orbite polaire a eu lieu en 2007. Depuis, les essais aux caractéristiques techniques parfois difficiles à interpréter ont eu lieu à un rythme soutenu. Pour la Chine, se doter d'une capacité ASAT permet surtout, dans un contexte de guerre psychologique, découplé des capacités réelles, de renforcer sa capacité dissuasive face aux États-Unis[33].

Ces capacités – couplées aux progrès accomplis dans le secteur de l'intelligence artificielle – sont utilisées à la fois dans des opérations de contrôle et de surveillance, de contre-propagande, mais également en support aux opérations militaires. Alors que les questions d'attribution ne sont pas levées, la zone grise des offensives sur le théâtre de la guerre de l'information cybernétique permet à moindre coût, selon les stratèges chinois, de conserver l'initiative et de renforcer la puissance de dissuasion

ou d'interdiction de la Chine face à tout adversaire potentiel[34]. La simple menace de dommages majeurs contre des installations vitales pourrait permettre, selon Pékin, de contrôler une escalade potentiellement défavorable aux forces chinoises.

Pour maîtriser le nouveau champ de bataille de la guerre de l'information, la Chine a entrepris la modernisation de ses capacités en matière de technologies de l'information, de l'informatisation des systèmes d'armes et des réseaux de communication et plus globalement de l'ensemble des capacités C3I puis C4I dès la fin des années 1990. Les lacunes étaient et sont encore considérables, notamment concernant l'imbrication de l'ensemble des capacités, que ce soit dans le domaine du contrôle à distance, de l'espace et des capacités informatiques, indispensables à l'amélioration des capacités de détection et de compréhension d'une situation donnée, ainsi qu'au bon fonctionnement des réseaux de communication en situation de combat[35].

En matière d'intelligence artificielle, qui permet aussi de démultiplier les capacités de l'APL dans tous les domaines, de l'entraînement au ciblage des attaques cybernétiques, la Chine ambitionne d'occuper une position de leadership à l'horizon 2030 et a adopté en 2017 un plan de développement de l'intelligence artificielle appliquée à l'ensemble des domaines civils et militaires[36].

Les réformes institutionnelles de l'APL mises en œuvre par Xi Jinping en 2015, tiennent compte de ces évolutions majeures et ont l'ambition de regrouper tous les éléments de la guerre de l'information sous un seul commandement[37]. Une Force de soutien logistique a été créée, au côté de la Force des lanceurs (nouvelle appellation de la Seconde artillerie)[38]. Dépendant de cette nouvelle force, le Network System Department a pour mission la guerre cybernétique, les technologies de reconnaissance, la guerre électronique et la guerre psychologique. Ces capacités sont intégrées

aux stratégies de déni d'accès que la Chine tente de développer face aux États-Unis[39].

Retour aux sources : la guerre du peuple appliquée à la guerre de l'information

La guerre de l'information « aux couleurs de la Chine » comporte également une dimension héritée de la tradition stratégique classique et maoïste. Les forces régulières sont complétées par des forces « irrégulières » et des milices populaires. Ces dernières, qui existent depuis les origines de l'Armée rouge, constituées de civils, viennent en appui des forces de l'APL pour des opérations de guérilla ou de soutien dans tous les secteurs.

Dans le domaine de la guerre de l'information, la « milice » des ingénieurs civils et des hackers « patriotiques » est pleinement mobilisée depuis 2002[40]. Les hackers civils fournissent les armées de trolls et les opérations de pénétration ou de submersion des réseaux ennemis. Les unités régulières, dépendant de l'APL, ont été accusées en 2012 par les États-Unis d'avoir lancé des offensives contre plus d'une trentaine de compagnies américaines, dont la compagnie de sécurité informatique Mendiant[41].

Créée en 2017, la commission pour l'intégration civile et militaire, avec à sa tête Xi Jinping, a pour mission d'offrir aux forces chinoises, dans la guerre de l'information, toutes les ressources du secteur civil, y compris les transferts de technologie et les coopérations scientifiques mises en place avec des entreprises et des centres de recherche étrangers. Au mois de décembre 2017 le Cyber Security Innovation Center a été inauguré, dont l'objectif est d'aider l'APL à « remporter les guerres de demain » en intégrant les domaines d'excellence de l'industrie civile[42]. Au mois d'octobre de la même année, la Cyberspace Administration of China (CAC)

publiait également un document appelant à renforcer l'intégration civile et militaire dans le domaine de la cybersécurité.

Le plan Chine 2025, présenté par le Premier ministre Li Keqiang en 2015, ciblait également un ensemble de domaines – dont les technologies de l'information – dont la principale caractéristique est la dualité des applications[43]. De même, le plan « 1 000 talents », présenté en 2008, visait à faciliter le retour et le recrutement des scientifiques les plus brillants formés à l'étranger. Il a été remplacé en 2019 par un nouveau programme de recrutement d'experts étrangers de haut niveau[44].

*

Profondément intégrée à la pensée militaire chinoise, de Sun Zi à Mao Zedong, et à la situation d'asymétrie de puissance dans laquelle se trouve encore l'APL face à la puissance militaire américaine, la guerre de l'information dans toutes ses dimensions – y compris celles de la propagande interne et externe – est donc au cœur du développement de la réflexion stratégique en Chine depuis le début des années 1990. Elle sert aussi de moteur au développement des capacités de l'APL, avec une systématisation de l'intégration des moyens civils et militaires. Si la Chine est loin d'avoir atteint le niveau de développement technologique des puissances occidentales en la matière, l'utilisation de moyens détournés et d'unités irrégulières, selon les principes de la guerre populaire, permettent aussi de démultiplier la capacité d'action défensive et offensive du régime dans un contexte où menace intérieure et menace extérieure sont – pour le régime chinois – étroitement imbriquées.

Pour aller plus loin

PILLSBURY Michael, *Chinese Ways of Future Warfare*, National Defense University Press, 1997.

QIAO Liang, WANG Xiangsui, *La Guerre hors limites* (1999), Rivages, Paris, 2003.

WOTZEL Larry, *The Chinese People's Liberation Army Information War*, US Army War College, 2014.

YIN J., TAYLOR P. M., « Information warfare operations from an Asian perspective », *Journal of International Warfare*, 2008, vol. 7, n° 1.

FOCUS 4

Taïwan : laboratoire des manipulations de l'information chinoises

Paul Charon

Lors de son audition devant le parlement taïwanais, le 2 mai 2019, Chen Wenfan (陳文凡), directeur adjoint du Bureau de la sécurité nationale (BSN), a déclaré que la Chine était parvenue à infiltrer le champ médiatique taïwanais par le truchement de ce qu'il a appelé des « médias conformes » (同路媒体). Contrôlés par Pékin, ces médias manipulent l'information afin de déconsidérer la présidence de Tsai Ying-wen et de démonétiser le système démocratique. Le BSN a qualifié ces opérations de guerre cognitive (认知作战)[1], dans le sens où elles ont pour ambition de forger un récit conforme aux intérêts de Pékin ; elles mettent en lumière, du reste, les efforts consentis par la Chine afin d'édifier un pouvoir discursif (话语权) qui lui permette d'imposer son discours sur la scène internationale, mais aussi de façonner les esprits dans des pays cibles.

Objectif prioritaire du pouvoir chinois, Taïwan a constamment fait l'objet d'efforts significatifs en matière d'opérations de Front uni afin de favoriser la réunification pacifique[2]. Mais la trajectoire singulière de l'identité locale, la démocratisation du régime et la restructuration du

système de partis ont éloigné cette perspective politique et contraint la Chine à repenser sa stratégie à l'égard de l'île : celle-ci repose désormais sur un large répertoire de modes d'action, au sein duquel les manipulations de l'information occupent une place essentielle.

La matrice doctrinale

Le recours aux opérations d'influence, y compris de désinformation, n'est pas chose nouvelle pour le régime chinois ; nombre de travaux ont souligné l'existence, dès la constitution des bases rouges à la fin des années 1920, d'une politique de propagande interne et externe particulièrement active[3]. Inspirées en partie de l'expérience soviétique en la matière, les opérations d'influence chinoises menées contre Taïwan puisent à deux sources doctrinales majeures : le Front uni (统一战线) et les « Trois guerres » (三种战法).

Le Front uni ne se limite pas à une simple coalition forgée avec des forces non communistes afin de conquérir le pouvoir et de faire advenir la révolution ; il a perduré bien après la révolution et consiste avant tout à « mobiliser les amis du Parti pour frapper ses ennemis[4] ». Cet outil destiné à façonner les forces externes au Parti a pris, à Taïwan, la forme d'une instrumentalisation des forces favorables à la réunification contre celles qui soutiennent l'indépendance. Le Front uni[5] est ainsi l'une des « trois armes magiques » (法宝) théorisées par Mao Zedong en 1938[6], les deux autres étant la lutte armée et la construction du Parti. Ces stratégies ne relèvent pas du seul département du Travail de Front uni, mais irriguent l'ensemble de l'appareil du Parti dont toutes les branches ont pour mission de mettre en œuvre cette politique.

La doctrine des « Trois guerres » a, quant à elle, été formulée en 2003 ; elle se compose de la guerre psychologique (心理战), de la guerre de

l’opinion publique (舆论战) et de la guerre du droit (法律战). Ces trois dimensions, qui visent respectivement à influencer les décisions de l’adversaire, à modeler son opinion publique et à forger un contexte légal favorable à la Chine, ne doivent pas être comprises comme une version chinoise de la guerre hybride, mais comme une continuité de l’action du Parti[7].

Bras armé du Parti communiste chinois (PCC), plutôt qu’armée nationale, l’Armée populaire de libération (APL) a en effet pour mission première d’assurer la pérennité du régime en décuplant le pouvoir politique du PCC. C’est dans ce cadre que doivent être interprétées les « Trois guerres » qui nourrissent les opérations menées à Taïwan par l’APL, notamment par la base 311 de Fuzhou située de l’autre côté du détroit et entièrement dédiée aux opérations informationnelles sur l’île[8].

Subvertir Taïwan

Pour ce qui concerne Taïwan, l’objectif de Pékin est moins désormais d’imposer une narration positive, que de faire éclater la société taïwanaise, et son régime démocratique, sous le poids de ses contradictions internes.

Les opérations d’influence chinoises se caractérisent par une approche holistique mêlant une multitude d’acteurs (relevant du Parti, de l’État et de l’armée auxquels sont associés des acteurs non étatiques) et différents vecteurs « recrutés » au sein de la société taïwanaise. Cette diversité de moyens assure à ces opérations une portée significative, malgré un manque de coordination manifeste. Une narration donnée, telle que la rumeur prétendant que la présidente Tsai Ing-wen ne serait pas véritablement titulaire d’un doctorat, peut ainsi être relayée par une multitude de vecteurs visant des segments spécifiques de la société taïwanaise.

Pékin s’appuie d’abord sur des médias traditionnels (presse, radio, télévision). Au-delà des grands acteurs du secteur (CGTN, *Global Times*, Xinhua, etc.) qui assurent la diffusion du point de vue chinois, les autorités chinoises recourent également à des médias prétendument indépendants. La base 311 de Fuzhou est ainsi dotée d’unités subalternes ou associées, donc relevant de l’APL, qui se font passer pour des médias privés et qui répandent à Taïwan une information conforme aux intérêts de Pékin. C’est le cas de Voice of the Strait (VTS), créée en 1958 (d’abord sous un autre nom) avec pour mission de diffuser la propagande communiste à Taïwan, mais aussi de structures moins connues et plus récentes, telles que la maison d’édition Haifeng qui publie des ouvrages destinés à forger une vision commune entre les deux rives.

La Chine s’est également employée à coopter des médias taïwanais susceptibles de relayer ses discours. En 2008, le groupe Want Want Holdings acquiert China Times group qui détient CTi TV et CTV[9], deux chaînes de télévision taïwanaises influentes. Le propriétaire de la holding, Tsai Eng-Meng (蔡衍明), est accusé par les autres médias taïwanais d’entretenir des liens étroits avec le PCC et de diriger des « médias rouges ».

Enfin, les médias sociaux sont de même mis à profit. Société extrêmement connectée, Taïwan ne peut être conquise sans le contrôle des récits qui se propagent sur les réseaux sociaux, notamment Facebook, Line, PTT et Instagram. La Chine a ainsi tenté, avec un succès limité, de racheter des pages Facebook de Taïwanais pouvant servir de support pour la publication de contenus fabriqués en Chine. Désireux de mieux atteindre les jeunes, les acteurs chinois de la désinformation ont coopté plusieurs *youtubers* et autres influenceurs chargés d’assurer la diffusion des récits préparés en échange, le plus souvent, de rétributions financières.

Lorsque le ralliement de ces médias s’avère impossible, Pékin n’hésite pas à menacer les leaders d’opinion qui propagent des contre-narrations

dérangeantes. J. Michael Cole, rédacteur en chef de *Taïwan Sentinel*, explique ainsi avoir été victime d'une campagne de dénigrement, en provenance de Chine, l'accusant d'être rémunéré par Tsai Ing-wen ou encore d'être un agent de la CIA [10].

Vers une complexification des opérations chinoises

L'une des faiblesses des opérations de désinformation chinoises tient à la difficulté manifeste des acteurs du continent à proposer des informations rédigées en caractères traditionnels, les logiciels de traduction automatique faisant souvent des erreurs. La Chine communiste a en effet « simplifié » une partie des caractères chinois dans les années 1950, tandis que Taïwan a conservé l'écriture traditionnelle. Shen Boyang (沈伯洋), enseignant à l'université Nationale de Taipei et fondateur du DoubleThink Labs, a montré comment Pékin apprend à contourner cette difficulté en faisant appel à des relais hors de Chine : des cabinets de relations publiques ou des agences marketing sis à Taïwan sont recrutés pour mener des campagnes commanditées par la Chine ; des fermes de contenus (内容农产) sont financées en Asie du Sud-Est, notamment en Indonésie qui accueille une importante diaspora chinoise. Cette complexification des opérations chinoises permet de produire des narrations moins « chinoises » aux yeux du public taïwanais et d'estomper les liens avec le commanditaire chinois [11].

La Chine a longtemps, et sans succès, parié sur la victoire du parti nationaliste (KMT), plus favorable à un rapprochement entre les deux rives. L'échec patent de cette approche l'a conduite à rechercher un contact direct avec les acteurs de la société civile taïwanaise et à renoncer aux intermédiaires dans ses opérations informationnelles. C'est la raison pour laquelle Pékin construit patiemment des réseaux d'influence auprès d'associations professionnelles (pêcheurs, fermiers, agriculteurs

notamment), de temples bouddhistes (tels ceux dédiés à la déesse Mazu dont le culte existe également en Chine, dans la province du Fujian), d'élus locaux, mais aussi de groupes criminels, qui sont autant de relais mobilisables pour la propagation des narrations fabriquées en Chine[12].

Enfin, la Chine a longtemps cherché avant tout à diffuser une image positive d'elle-même. Elle croyait que cette approche serait suffisante pour rallier la population taïwanaise à la mère-patrie. L'échec de cette « stratégie de séduction » a conduit Pékin à suivre la voie empruntée par Moscou après la guerre de Géorgie d'août 2008[13]. Faute de pouvoir conquérir les « cœurs et les esprits », Pékin a embrassé pleinement la stratégie russe consistant à identifier, puis à amplifier, les fractures internes des sociétés cibles[14]. Or, la société taïwanaise est travaillée par des clivages profonds et pâtit d'une polarisation politique relativement forte. La démarche de Pékin vise ainsi, en attisant les tensions, à accroître le sentiment de défiance à l'égard d'un système démocratique incapable de produire suffisamment de lien social. La nouvelle stratégie chinoise à Taïwan est donc bien celle d'une « libanisation », comme l'affirme J. Michael Cole, en ce qu'elle aspire à morceler la société[15]. Ce travail de sape doit *in fine* conduire à la réunification pacifique des deux rives ou à l'affaiblissement de l'esprit de défense face à une invasion de la Chine.

*

Quoique soutenu militairement par les États-Unis, Taïwan n'est reconnu que par 15 États et exclu de la plupart des organisations internationales ; son isolement diplomatique est donc particulièrement prononcé. Abandonné, seul ou presque face aux ambitions chinoises, Taïwan peut être considéré comme un laboratoire où Pékin met à l'épreuve l'efficacité de ses opérations informationnelles. Les expérimentations chinoises à Taïwan devraient alarmer les démocraties pour deux raisons au moins : d'abord, les manœuvres chinoises mettent en péril le système politique de Taïwan qui

compte parmi les rares démocraties de la région Asie Pacifique. Ensuite, ces manipulations de l'information chinoises, resserrées géographiquement pour l'heure sur Taïwan (et Hong Kong), semblent en passe de s'étendre à d'autres parties du monde. Un faisceau d'indices, particulièrement inquiétants, observables au Canada, en Australie, en Europe et en Afrique, révèle en effet que Pékin est d'ores et déjà engagé dans une entreprise de mondialisation de ses opérations de manipulation de l'information.

CHAPITRE 6

Corée du Nord : la stratégie informationnelle de Kim Jong-un

Marianne Péron-Doise

Les interrogations sur la résilience du régime nord-coréen et le scénario d'un inévitable effondrement nourrissent la littérature consacrée aux évolutions stratégiques de la péninsule coréenne depuis les années 1990. Il est vrai que l'arrêt de l'aide soviétique suivie de l'épisode de famine généralisée qui a affecté le pays a suscité bien des analyses pessimistes. Pour autant, 70 ans après sa création, le régime nord-coréen s'est maintenu sans dévier de sa ligne idéologique initiale, le *juche*, ou autosuffisance. Qui plus est, il est resté aux mains d'une même famille. L'actuel dirigeant, Kim Jong-un, à la tête du pays depuis 2012, est le petit-fils du fondateur de la République populaire démocratique de Corée, Kim Il-sung, à qui son fils, Kim Jong-il, avait succédé à sa mort en 1994.

La crise nucléaire a accentué la mise à l'écart du pays en raison de l'imposition de sanctions dès 2006. Elle a servi à renforcer le sentiment identitaire de la population et à expliquer les difficultés du quotidien. Selon cette logique, tout doit être sacrifié au développement d'un programme nucléaire et balistique destiné à protéger le pays d'un environnement

hostile. L’arme nucléaire obéit ainsi à une logique intérieure propre à asseoir la légitimité du régime et la puissance de son dirigeant, objet d’un culte de la personnalité savamment orchestré par l’appareil de propagande du régime tant à l’intérieur qu’à l’extérieur du pays. La quasi-immuabilité du système politique du pays s’explique en partie par ses ressorts sécuritaires, son nationalisme intransigeant, mais aussi par son contrôle absolu sur l’information[1].

Les ressorts informationnels d’une idéologie totalitaire

La manipulation continuelle de l’histoire a enfermé le pouvoir nord-coréen dans sa lecture paranoïaque des relations internationales et la perception que ses voisins ne souhaitent que sa disparition et qu’ils travaillent à l’affaiblir. Pour Pyongyang, les États-Unis et ses proches alliés sud-coréens et japonais préparent des scénarios d’invasion sous le prétexte d’entraînement et d’interopérabilité. Le Comité central du Parti des travailleurs de Corée dispose d’un département du Front uni, chargé d’organiser des opérations de guerre psychologique contre l’extérieur, notamment la Corée du Sud, et de laisser planer la menace d’une réunification par la force. Pendant la guerre froide, les stratégies de contre-influence pour décrédibiliser le régime de Séoul, présenté comme corrompu et inféodé aux États-Unis, étaient très efficaces et trouvaient un écho auprès des pays frères du bloc de l’Est. Après l’effondrement de l’URSS, et le déclin de l’économie nord-coréenne provoqué par la fin de l’aide soviétique et des pays satellites, la stratégie s’est inversée pour se tourner davantage vers la population nord-coréenne[2].

L’idéologie du régime s’articule autour du dirigeant et de sa famille dont les statues et les portraits se dressent dans tout le pays *via* un ensemble de relais informationnels et de supports disponibles[3]. Ce culte de la personnalité fait du dirigeant suprême un visionnaire, un sage omniscient qui a réponse à tout. Ainsi Kim Jong-un, et avant lui son père et son grand-père, sont généralement représentés visitant un site militaire, une usine ou une ferme collective entourés d’accompagnateurs qui tiennent en main un carnet et un crayon afin de noter les recommandations qui ne manqueront pas d’améliorer la productivité du lieu. Kim Il-sung, héros de la guerre de libération contre le colonisateur japonais, porte le titre de « Président éternel ». Déifié, il repose dans un mausolée où une foule ininterrompue de Nord-Coréens, écoliers en tête, vient lui rendre hommage. C’est à son initiative qu’a été édifié, dans les années suivant la guerre de Corée, le village modèle de Kijong-Dong dit « village de la paix », à la frontière entre les deux Corées. Censé abriter deux cents habitants et projeter une image de la prospérité socialiste, il se révélera inhabité. Séoul le rebaptisera « village de la propagande » en raison de sa facticité, de la présence d’un mât de 160 mètres de haut arborant un drapeau nord-coréen et de haut-parleurs diffusant en continu et à pleine puissance des diatribes antiaméricaines et anti-sud-coréennes alternant avec des chants patriotiques nord-coréens[4].

Le nationalisme identitaire, forgé pendant la guérilla antijaponaise, puis pendant la guerre de Corée, est un ressort privilégié du régime, comme dans tout système totalitaire qui a besoin d’un « ennemi ». Les services d’information nord-coréens diffusent ainsi les images d’un pays militairement puissant et fier, bravant les États-Unis en s’appuyant sur un leadership fort et respecté. Leur narratif stratégique est de mettre en scène le *hard power* nord-coréen, c’est-à-dire sa résolution à se défendre et au besoin à prendre l’initiative d’une attaque préemptive.

Ce message d’intimidation, associé aux essais nucléaires et balistiques répétés du régime, notamment sous Kim Jong-un, a quasiment neutralisé

toute perspective d'une option militaire. Les États-Unis et la Corée du Sud ne veulent pas courir le risque d'une frappe nucléaire dont le coût politique et humain serait élevé. Le dilemme de sécurité de la péninsule coréenne tourne entièrement autour de l'incertitude stratégique que Pyongyang entretient depuis des années sur ses capacités militaires et ses intentions réelles.

Des affiches de propagande stigmatisant une menace américaine omniprésente galvanisent la loyauté de la population. En septembre 2017, après le discours du président Trump à la tribune des Nations unies au cours duquel il a menacé de détruire la Corée du Nord, une campagne d'affiches particulièrement agressives, dont celle de missiles détruisant le siège du capitole à Washington, avait été lancée dans tout le pays et était visible sur le site Internet de *Voice of Korea*[5]. Toutefois, à partir des rencontres au sommet entre le dirigeant nord-coréen et le président américain[6], en 2018, elles ont été moins présentes dans les rues de Pyongyang. De même, la Corée du Sud a été présentée sous un jour plus positif à partir de la séquence de réchauffement des relations intercoréennes. Ainsi, le thème de la réunification, symbolisé par une carte de la Corée en bleu sur fond blanc était visible dans tout le pays en 2018. Il a été repris dans des spectacles de masse organisés à Pyongyang cette même année, tandis qu'un écran géant projetait les images de la rencontre de Panmunjon de septembre 2018 entre le président sud-coréen Moon Jae-in et son homologue nord-coréen[7].

Les leviers techniques de l'autarcie informationnelle

L'agence de presse centrale nord-coréenne, Korean Central News Agency (KCNA)[8] a le monopole de l'information qu'elle diffuse

quotidiennement à l'intérieur et à l'extérieur du pays, *via* son site Internet et la télévision d'État, Korea Central Television (KCTV). Fondée en 1946, l'agence publie dans la langue nationale mais aussi en chinois, en japonais, en espagnol et en anglais. Son édition anglaise en fait le principal outil d'influence du régime à destination de l'étranger. Ses informations sont reprises par différents sites dont *Uriminzokkiri*[9] (우리민족끼리), qui diffuse des actualités nord-coréennes dans trois langues, le coréen, le russe et l'anglais, mais aussi des journaux, tels le *Rodong Sinmun*, organe du Parti des travailleurs de Corée, ou le *Pyongyang Times*.

Le régime communique également *via* des comptes Twitter ou YouTube, où il publie des images et des vidéos retransmettant des défilés militaires, et où il diffuse les tirs balistiques et nucléaires auxquels il procède. Convaincue de la puissance de l'image, la Corée du Nord a lancé, en mars 2019, un nouveau site Web qui reprend les nouvelles du journal du Présidium de l'Assemblée populaire suprême, le *Mingu Chosun*[10].

La mainmise étatique sur l'information qui s'exerce sur la population et sur l'extérieur du pays permet la manipulation des idées et la distorsion de la réalité politique ou historique. Il en résulte une société nord-coréenne monolithique, très encadrée et soumise à une mobilisation idéologique continue à tout âge, dans toutes les sphères des activités sociales. La vision du monde de l'État occupe tout l'espace public et privé.

Un desserrement du contrôle de l'information a été enregistré dans les années qui ont suivi la famine de 1996-1997. Le relâchement de la surveillance aux frontières avait permis à de nombreux Nord-Coréens de se rendre en Chine en quête de nourriture et de médicaments. Cette période a vu la création d'une économie parallèle et de marchés privés tolérés par le régime. Si les allées et venues transfrontalières ont favorisé le développement de trafics et de pratiques de corruption, elles ont également eu pour effet d'introduire sur le marché noir des supports techniques, tels

des cassettes ou des DVD révélant l'existence d'autres modes de vie et une image différente de la Corée du Sud que celle véhiculée par le régime [11].

La circulation de clés USB de contre-propagande introduites clandestinement par des réseaux d'activistes sud-coréens a pu, de la même façon, contribuer partiellement à cette prise de conscience. Ces deux phénomènes conjugués ont révélé la faillite sociale et économique du régime et permis l'avènement d'une nouvelle génération de Nord-Coréens, la génération *Jangmadang* (장마당), moins perméable à l'idéologie et ayant davantage d'attentes en matière de confort et de niveau de vie [12]. C'est à cette génération que semble désormais s'adresser le régime, soucieux de susciter les bases d'un nouveau contrat social avec la population.

La Corée du Nord n'est pratiquement pas reliée à l'Internet mondial. Elle possède un réseau national, un Extranet séparé, pour certains citoyens, le ministère de la Sécurité du peuple, le ministère de la Sécurité de l'État et les militaires. L'Extranet non classifié *Kwangmyong* (광명), relie 3 700 organisations à 50 000 usagers estimés pour une population de 25 millions d'habitants. La plupart des ordinateurs nord-coréens utilisent le système d'exploitation Red Star, développé localement et fondé sur un software ouvert, Linus, et disposent d'un moteur de recherche appelé Naenara (내나라) [13]. Les câbles de fibre optique apportant Internet proviennent de Chine et utilisent des adresses IP chinoises. L'accès n'est pas régulier en raison d'un réseau électrique peu performant [14]. Les autorités nord-coréennes se montrent réticentes à favoriser l'accès à Internet, bien que très réduit et sous contrôle, privant le pays d'opportunités de commerce et d'échanges qui permettraient de contourner les sanctions et d'aider à sa survie économique.

L'information comme vecteur d'« ouverture »

Depuis l'arrivée de Kim Jong-un au pouvoir en 2012, la Corée du Nord montre des signes de changement tant sur le plan intérieur que sur le plan extérieur. Épris de modernité, le jeune dirigeant s'est saisi de l'information pour en faire le symbole de sa volonté de réforme. Si l'accès aux ordinateurs reste sévèrement réglementé, ceux-ci sont visibles dans les lieux publics, comme les universités, les centres de documentation, les magasins, les restaurants et les hôtels.

L'usage du téléphone portable s'est généralisé en ville, comme à la campagne, depuis son introduction en 2002 puis la constitution d'un réseau de télécommunications sous strict contrôle d'État, Koryolink (고려링크), après la constitution en 2008 d'une *joint-venture* entre la compagnie publique de télécommunications nord-coréenne, Korea Posts and Telecommunications (KPTC), des entreprises chinoises et une société de téléphonie égyptienne, Orascom[15]. Importés de Chine, les téléphones portables recourent à la 3G. Le nombre des usagers estimé à 2,5 millions, soit 10 % de la population en 2012, a progressé[16]. Ces derniers peuvent consulter les actualités diffusées par le journal officiel du régime *Rodong Sinmum*, la météo, écouter de la musique, jouer, et disposent de réseaux sociaux[17]. Les portables comprennent un système de surveillance permettant aux autorités de contrôler les appels et les transmissions de données.

Le contact avec les étrangers est devenu plus aisé avec le développement du tourisme. Source de devises, le tourisme permet aussi à la Corée du Nord de projeter une image de modernité et de s'essayer au *soft power*. Cette politique d'ouverture vise notamment à contrebalancer l'image négative dont le régime souffre à l'international et à poursuivre le processus de normalisation diplomatique amorcé avec la succession de rencontres au sommet effectuées par Kim Jong-un depuis 2018, dont l'emblématique rencontre de Singapour avec l'ennemi d'hier, le président américain, Donald Trump, le 12 juin 2018.

Aujourd'hui les actions d'influence du régime se font plus subtiles : elles cherchent à modeler la stature d'homme d'État du jeune dirigeant en le présentant comme une personne rationnelle et recherchée. La télévision et les médias gouvernementaux retransmettent avec force détails les visites de Kim Jong-un à l'extérieur du pays et les entretiens avec des puissances internationales de premier rang, comme les États-Unis, la Chine et la Russie, et avec des puissances régionales, comme la Corée du Sud, Singapour et le Vietnam.

La plus grande menace contre l'hégémonie informationnelle de l'État est représentée par l'accès aux téléphones portables. En dépit de ses moyens de surveillance électronique sur l'ensemble des nouvelles technologies d'information introduites dans le pays, le gouvernement ne peut plus procéder à une surveillance de la population aussi étroite qu'auparavant.

Avec l'usage du téléphone portable, la capacité à créer des relations horizontales, de personne à personne, voire de constituer des groupes d'échanges en réseau hors des cadres collectifs réglementés par l'État et le Parti, a créé une dynamique interne mettant fin à l'isolement des individus. À terme, cette capacité à s'organiser sur une base sociale choisie peut contribuer à une lente, mais réelle, mutation de la société nord-coréenne dans son rapport à l'État et au monde qui l'entoure [18].

L'information et le cyber comme outils de guerre

En l'espace de dix ans, la péninsule coréenne a dû intégrer des menaces hybrides et multidimensionnelles. Les scénarios de crise liés à un conflit conventionnel de haute intensité comprenant des menaces nucléaires, balistiques, chimiques ont évolué vers un ensemble de défis de nature asymétrique, telles des guerres informationnelles et de possibles cyberattaques. Cette évolution reflète la culture stratégique nord-coréenne

qui consiste à s'appuyer sur des capacités asymétriques afin de compenser son retard technologique croissant dans le domaine conventionnel face à l'alliance américano-sud-coréenne.

Pour certains analystes, les deux Corées sont engagées dans des conflits informationnels ayant trois finalités : obtenir des renseignements sur leurs stratégies et capacités respectives ; protéger leurs systèmes d'information, tout en cherchant à neutraliser et à détruire celui de l'adversaire ; enfin, lancer des opérations de désinformation afin de modeler leurs narratifs stratégiques internes et externes[19]. La guerre de l'information qu'elles se livrent associe ainsi le renseignement, le cyber et la désinformation.

En plus de posséder des armes de destruction massive, la Corée du Nord représente désormais une menace cyber significative. Ce nouveau défi met à l'épreuve la stratégie de défense et les concepts opérationnels des États-Unis et de ses alliés dans la région. La Corée du Nord mise sur le cyber car elle estime être peu vulnérable dans ce domaine. Aussi se déclare-t-elle en train de préparer une guerre de « quatrième génération » en établissant des unités de *cyber-warfare*.

Les capacités nord-coréennes dans le domaine cybernétique sont plus avancées que ne le laisseraient supposer la faiblesse de l'économie nationale, les défaillances du réseau électrique et l'usage restreint d'Internet. Il fait peu de doute que le régime a acquis de nouvelles capacités de nuisance grâce au cyber en se plaçant désormais dans le registre offensif de la cybercoercition, comme le définit un rapport de la RAND[20].

Beaucoup d'attaques lui sont publiquement attribuées, tant par les États-Unis que par la Corée du Sud. Une signature nord-coréenne aurait été décelée derrière des attaques à l'encontre des studios Sony en 2014 ou lors de l'épisode Wannacry[21] qui a totalement paralysé le système de santé britannique en 2017 et qui a été attribué par de nombreux pays et par le Trésor américain au groupe de hackers Lazarus[22]. Ce logiciel malveillant de type rançongiciel (*ransomware*) a défrayé la chronique en 2017 en infectant

plus de 230 000 ordinateurs dans le monde dont ceux de beaucoup d'agences gouvernementales et d'hôpitaux. Le virus prenait en otages des données personnelles et exigeait une rançon en bitcoins pour leur déchiffrement. En septembre 2019, le Trésor américain a mis en place des sanctions contre trois groupes de hackers dont il a été établi qu'ils travaillaient pour le gouvernement nord-coréen en raison de leur lien direct avec le Bureau de reconnaissance générale (BGR), l'institution principale du Parti des travailleurs de Corée en charge du renseignement. Outre Lazarus, le rapport mentionne les groupes Bluenoroff et Andariel, et évoque leurs activités criminelles en soutien au développement des programmes d'armes nord-coréens.

Contrairement aux pratiques russes ou chinoises, les opérateurs nord-coréens font peu d'efforts pour dissimuler leurs opérations[23]. Deux tendances majeures caractérisent les opérations nord-coréennes : le choix de cibles faiblement défendues qui permettent de collecter beaucoup d'argent afin d'augmenter les revenus d'un gouvernement nord-coréen affaibli par le régime des sanctions mis en place depuis 2006 et le développement de techniques à l'effet déstabilisant global avec des logiciels malveillants. Outre la captation financière, les actions cybernétiques offensives visent des objectifs militaires avec une recherche active de déstabilisation et de renseignement, ou peuvent servir des intentions idéologiques. Dans ce dernier cas, les opérations d'influence cherchent à décrédibiliser les régimes américain, sud-coréen et japonais ou à discréditer des « défecteurs », c'est-à-dire des citoyens qui ont réussi à s'enfuir de Corée du Nord en passant au sud.

Au sein de l'Armée populaire nord-coréenne, le BGR ainsi que le département de l'État-major général (DEMG) sont les deux entités chargées de contrôler et d'orienter les activités cyber nord-coréennes[24]. En temps de paix, le BGR entretient un climat d'instabilité en recourant à des actions d'éclat et à des provocations (infiltrations, raids de commandos). Ainsi, on

lui attribue le torpillage d'une frégate de la marine sud-coréenne *Cheonan* qui a fait plus de 40 morts en mars 2010. En temps de guerre, le DEMG est chargé de la planification d'opérations d'influence actives.

Face aux cyberattaques nord-coréennes se pose le problème de l'attribution publique. Un certain niveau de discrétion est parfois préféré par les cercles gouvernementaux de crainte d'être pris pour cible. Pour des raisons de sécurité, les planificateurs militaires américains et sud-coréens ont préféré taire les tentatives d'intrusions réussies d'opérateurs nord-coréens. Ceux-ci auraient pu avoir accès à des plans d'opérations sensibles par le piratage de données informatiques[25].

Cependant, la Corée du Sud envisagerait de lancer des contre-attaques contre le Nord en prenant le contrôle de son Intranet pour y disséminer des informations démentant la propagande officielle. Après l'épisode tragique du torpillage du *Cheonan*, les forces américano-sud-coréennes se sont engagées dans une séquence active de guerre psychologique. Les autorités militaires sud-coréennes ont créé une nouvelle unité *psy-ops* chargée de diffuser des actualités et des informations en Corée du Nord, en utilisant des transmissions radio, des ballons gonflables acheminant des tracts, des DVD et des clés USB. L'effet de ces initiatives de contre-information sur la société nord-coréenne reste difficile à évaluer. Elles sont cependant redoutées par Pyongyang qui les dénonce régulièrement[26].

*

Depuis la fin de la guerre de Corée et la signature en 1953 d'un armistice – et non d'un traité de paix – entre les protagonistes, la péninsule coréenne est placée sous le signe d'une grande incertitude stratégique que la propagande nord-coréenne exploite avec efficacité. Sa politique de désinformation agressive s'appuie sur des provocations militaires incessantes, dont la recherche de capacités balistiques et nucléaires. L'arsenal des capacités nord-coréennes inclut aussi le risque cybernétique.

Cette intimidation permanente par différents moyens entretient un climat belliqueux avec des menaces de guerre qui sont prises très au sérieux par Séoul, Washington et Tokyo. Ces menaces n'étant pas uniquement verbales, elles ont un effet réel sur les politiques de défense et la diplomatie américaines, sud-coréennes et japonaises, y compris celles des soutiens chinois et russes de la Corée du Nord. En effet, l'ensemble de ces pays ne peuvent que se sentir concernés et alarmés par la perspective d'une crise majeure affectant la péninsule coréenne et de ses effets déstabilisants sur leurs populations et leurs économies.

Pour aller plus loin

FIFIELD Anna, *The Great Successor : The Secret Rise and Rule Of Kim Jong-Un*, Londres, John Murray, 2019.

KIM Insoo, « Interpreting North Korea's intentions : Use of vocal and visual code in TV message », *The Korean Journal of Defense Analysis*, décembre 2017, vol. 29, p. 533-550.

KIM Jina Kim, *The North Korea Nuclear Weapons Crisis : The Nuclear Taboo Revisited ?*, Basingstoke, Palgrave Macmillan, 2014.

LANKOV Andrei, *From Staline to Kim Il-Sung : The Formation of North Korea*, New Brunswick, Rudgers University Press, 2002.

PONS Philippe, *Corée du Nord : un État-guérilla en mutation*, Paris, Gallimard, 2016.

CHAPITRE 7

L’Iran : stratégie asymétrique et diplomatie de masse

Pierre Pahlavi

« Élevez vos paroles, pas votre voix. C’est la pluie qui fait pousser des fleurs, pas le tonnerre », écrivait le poète mystique persan du XIII^e^ siècle, Djalāl ad-Dīn Muhammad Rūmī, rappelant la place centrale qu’occupe le *soft power* dans la psyché collective et la culture stratégique des Iraniens. Sujets à un sentiment d’encerclement géopolitique, ces derniers sont convaincus que, en politique intérieure ou extérieure, l’esprit de conquête se conjugue avec la conquête des esprits. Souvent menacés et placés en infériorité militaire au cours de leur histoire, ils ont su mettre en œuvre l’approche asymétrique développée autrefois par les Ismaéliens et les Parthes, esquivant le combat frontal et portant les coups là où on ne les attendait pas pour mieux survivre et faire valoir leurs intérêts. Du *taqia* au *ketman* en passant par le *khod’eh* et le *tārof*[1], ils ont puisé dans l’attirail de feintes et de ruses accumulées depuis des siècles sur les champs de bataille, les arrière-cours des palais et les entrepôts des bazars.

Le grand jeu d’influence du XIX^e^ siècle et la grande révolution de l’information du XX^e^ siècle ont renforcé la certitude des dirigeants iraniens

que le sort de l’Iran se joue pour une large part sur le front des médias et des opinions publiques. Pendant la guerre froide, le régime monarchique s’était déjà doté d’un organisme de radiodiffusion appelé la Radio et télévision nationale iranienne (RTNI) pour promouvoir son image et soutenir ses objectifs de politique étrangère. Après la révolution islamique de 1979, le nouveau régime a réformé la RTNI pour créer le Sāzmān-e Sedā va Sima-ye Jomhūrī-ye Eslāmī-ye Īrān ou Islamic Republic of Iran Broadcasting (IRIB) et a entrepris une multitude d’initiatives médiatiques, culturelles, éducatives et religieuses afin de faire la promotion du régime et de ses valeurs.

L’arme informationnelle au cœur d’une stratégie globale

La guerre Iran-Irak, la guerre du Golfe et l’affirmation de la suprématie américaine ont fini de convaincre les dirigeants iraniens que la République islamique ne pouvait rien espérer de la confrontation directe avec ses adversaires régionaux et extrarégionaux et qu’elle devait investir dans une approche asymétrique faisant la part belle à l’influence médiatique et à l’arme informationnelle. Pour cela a été développée une stratégie à 360 degrés destinée à compenser les carences relatives de l’Iran dans les domaines diplomatiques, économiques, militaires. L’une de ses facettes consiste en une diplomatie publique sophistiquée qui passe par des canaux officiels et, de plus en plus, par l’intermédiaire de partenaires privés et étrangers permettant à l’Iran de faire fructifier son empreinte informationnelle sur l’échiquier international tout en restant sous le seuil de la violence.

Une vision du monde placée sous le mode obsidional

Motivée par l'ambition de voir l'ancienne Perse retrouver sa place dans le panthéon des grandes puissances, la politique étrangère iranienne l'est aussi, et sans doute davantage encore, par un profond sentiment de fragilité géopolitique découlant de la succession quasi ininterrompue d'ingérences de toutes sortes qu'a connue le pays au cours des siècles. Des conquêtes macédoniennes à l'opération Stuxnet de 2010, les interférences qui ont ponctué leur histoire plurimillénaire ont cultivé chez les Iraniens et leurs dirigeants un syndrome de citadelle assiégée auquel les géopoliticiens donnent le nom de « complexe d'obsidionalité », à savoir l'impression d'être enclavés dans un environnement régional et international particulièrement hostile.

Trait que confirme François Thual : « L'Iran a toujours perçu sa position géopolitique sous le mode obsidional, dans l'appréhension constante des menaces que font peser sur lui les États ou les nations qui l'entourent[2]. » Seul pays persan et chiite dans un voisinage à majorité turco-arabe et sunnite, note Shireen Hunter, l'Iran ne peut compter, face aux menaces extérieures, sur aucune solidarité ethnoculturelle naturelle[3]. À ces raisons de l'isolement iranien s'en ajoute une autre : le pays est à la fois trop grand et trop petit. Trop grand pour ne pas attiser la convoitise des poids lourds du jeu international. Trop petit – et donc trop faible – pour inhiber leurs appétits.

De ce double sentiment de fragilité et de solitude stratégique émanent deux impératifs stratégiques : protéger la « forteresse iranienne » en préservant son autonomie économique et son intégrité territoriale tout en projetant hors de ses enceintes son influence à l'échelle régionale afin de constituer une sphère d'influence protectrice. Deux réflexes apparemment contradictoires qui se complètent en réalité : « Si l'Iran brave la communauté internationale c'est qu'il sait que l'enjeu est la sanctuarisation de l'État-nation iranien prélude à une nouvelle phase d'expansion

idéologique[4]. » La politique étrangère de l'Iran trouve toute sa cohérence dans la poursuite de cette double ligne stratégique qui transcende les clivages idéologiques et s'incarne aussi bien dans l'approche offensive (*tahājomi*) d'un Ahmadinejad que dans la stratégie de détente (*tashanojzedāi*) d'un Rohāni[5].

De la dissymétrie à l'asymétrie : l'information comme arme stratégique

Sans conteste, la propagande (*tablighat*) et ce que l'on appelle aujourd'hui la diplomatie publique sont des « éléments-clés » pour la survie et la promotion des intérêts du régime islamique[6]. Mais, si l'adoption de l'arme informationnelle répond aux impératifs stratégiques de sa politique étrangère – protection de la souveraineté nationale et projection de son influence régionale – elle découle également de la lecture qu'ont fait ses dirigeants du rapport de force qui s'installe au lendemain de la guerre froide. Au sortir de la guerre Iran-Irak et de la guerre du Golfe, constatant ses propres faiblesses et la dissymétrie de la distribution de puissance à l'échelle internationale au profit des États-Unis et de leurs alliés occidentaux, le régime se tourne vers une conception asymétrique de la stratégie[7]. À l'instar de la Russie et de la Chine, l'Iran décide au début des années 1990 de miser sur cette approche multifacette qui consiste à compenser ses carences relatives dans les domaines diplomatiques, économiques, militaires en combinant tous ses atouts de manière prudente, pragmatique et non conventionnelle – c'est-à-dire en évitant soigneusement la confrontation directe avec ses adversaires américains, israéliens et arabes[8].

Il faut cependant attendre le début des années 2000, dans un contexte marqué par l'ascendant du Corps des Gardiens de la révolution (CGRI – ou en persan : Sepāh-e Pāsdārān-e Enghelāb-e Eslāmi), pour que la doctrine de

stratégie asymétrique de l'Iran arrive à maturité et soit véritablement institutionnalisée. En 2005, l'ayatollah Khamenei ordonne à ses principaux responsables de formuler une doctrine militaire dont la responsabilité et la conduite seront confiées aux Pasdaran[9]. Peu de temps après, le CGRI propose une stratégie de défense avancée (*forward defense*) fondée sur une logique multidimensionnelle à laquelle les autorités iraniennes donnent parfois le nom de *Doctrine Mosaïque*[10]. En septembre 2007, l'un de ses principaux concepteurs, le général Mohammad Djafari, alors directeur du centre stratégique du CGRI, explique que : « Compte tenu de la supériorité numérique et technologique de "l'ennemi", les forces iraniennes utiliseront des capacités de guerre asymétrique telles que celles utilisées par le Hezbollah lors du conflit de 2006 avec Israël au Liban. » Djafari, qui a commandé le CGRI de 2007 à 2019, ajoute alors que l'approche asymétrique iranienne doit s'articuler autour « des forces et des faiblesses » des puissances occidentales[11]. Dan Dickerson résume bien la portée de cette doctrine : à travers son adoption, l'Iran place sa rivalité avec l'Occident non pas sur le plan d'une opposition strictement militaire mais sur le plan d'un conflit global et intégré, d'une partie d'échecs à plusieurs niveaux incluant la compétition sociale, économique, idéologique et informationnelle[12].

Étant donné que le principal avantage comparatif des États occidentaux réside dans leur suprématie militaire, l'une des caractéristiques majeures de l'approche adoptée par Téhéran consiste précisément à éviter la confrontation armée directe à travers des approches de contournement non létal – d'où le nom de « stratégie sous le seuil de la guerre » (*short-of-war strategy*). Son but est de promouvoir les intérêts iraniens en agissant sous le radar et en évitant ainsi des frictions directes susceptibles de déboucher sur des conflits ouverts. Convenant, comme le lieutenant-général H. R. McMaster, qu'il n'y a que deux façons d'affronter les puissances occidentales – « *stupid and asymmetrically* » –, l'Iran, comme d'autres outsiders eurasiatiques, en est venu à la conclusion que la meilleure manière

de le faire est « de ne pas faire la guerre du tout, d'éviter autant que possible de faire usage de la force militaire et d'utiliser d'autres moyens pour tenter d'atteindre des objectifs qui ne pouvaient être atteints précédemment que par la victoire sur le champ de bataille[13] ».

Le résultat est une stratégie à 360 degrés déployée sur tous les plans et s'appuyant sur des moyens aussi divers que la diplomatie classique, les communications stratégiques, l'utilisation des diasporas, le terrorisme, l'exploitation de réseaux criminels ; tous les moyens permettant de rivaliser avec les puissances « conventionnelles » sur des « rings alternatifs » où leur supériorité est diminuée voire annulée. Informelles et ambiguës, ces stratégies multidimensionnelles sont conçues pour défier ces acteurs dominants en « semant la confusion et la méfiance » et en « usant la volonté de leurs opinions publiques »[14]. Dans cette logique, la propagande (*tablighat*), la désinformation, la (contre-)subversion ou la manipulation de l'information occupent une place de choix. Comme le souligne Withers, ces armes informationnelles tendent même à devenir prioritaires parce qu'elles permettent d'exploiter au maximum toutes les vulnérabilités du camp adverse tout en évoluant en « zone grise » et en demeurant sous le seuil du conflit généralisé[15].

L'influence du Corps des Gardiens de la révolution islamique

En raison du rôle qu'il joue dans la conception et la mise en œuvre de la stratégie asymétrique de l'Iran, le Corps des Gardiens de la révolution islamique (CGRI) exerce également une influence prépondérante sur sa facette informationnelle ; une influence qui s'est accrue au fur et à mesure que les Pasdaran se sont imposés, surtout depuis 2005, comme les véritables responsables de la politique interne et externe de la république islamique[16].

Sur le plan interne, le principal objectif du CGRI sur le terrain informationnel est de lutter contre ce que ses dirigeants appellent les « révolutions de couleur » et les tentatives de « coup d'État en douceur » fomentées, selon eux, par les adversaires régionaux et extrarégionaux du régime[17]. C'est dans cette optique que le gouvernement iranien accuse régulièrement les GAFA, comme Facebook ou Twitter, de soutenir la « propagande antirégime[18] ». Le Sepāh-e Pāsdārān supervise la lutte antisubversive au moyen d'un système de communication moderne utilisé pour éteindre la « sédition » et rallier l'opinion publique autour du régime[19].

Initialement limité à un outillage sommaire de propagande archaïque, cet effort d'encadrement doctrinaire de la population iranienne s'appuie sur un véritable arsenal de guerre psychologique moderne dont le Bureau du guide suprême, implanté au sein du CGRI, est l'un des principaux rouages. Créé de manière *ad hoc*, ce bureau devient rapidement un centre névralgique équipé de son propre organe de presse – le magazine mensuel *Sobhe-e Sadegh* –, ainsi que d'un réseau d'instituts culturels et de think tanks cogérés avec le ministère de la Culture, l'Organisation de la propagation de l'islam et l'agence d'information de la République islamique, connue sous l'acronyme IRIB. Dans le même ordre d'idées, le Sepāh-e Pāsdārān exerce une emprise plus ou moins directe sur de nombreux médias d'opinion. Ainsi l'influent journal *Keyhān* et le très puissant IRIB sont habituellement dirigés par des individus issus des rangs des Gardiens. Ces outils, combinés à l'exploitation des réseaux sociaux, servent la propagande interne pour assurer le soutien de l'opinion publique envers la République islamique[20].

Sur le plan externe, l'usage des communications stratégiques s'intègre pleinement dans l'approche asymétrique adoptée pour étendre l'influence iranienne et lutter contre celle des puissances régionales et extrarégionales[21]. Très tôt, les Pasdaran s'investissent dans la conduite d'actions subversives hors Iran au nom de la protection des peuples

« opprimés » par l'impérialisme[22]. Au cours des dernières décennies, les Gardiens de la révolution ont intégré à leurs méthodes l'utilisation des médias et des réseaux de communication pour atteindre les objectifs politiques suivants : dissuader leurs adversaires en brouillant les pistes et en les désinformant quant à leurs capacité et intentions réelles tout en ciblant leurs opinions publiques comme moyen indirect d'influencer l'action de leur gouvernement[23]. Comme le note Arsali, les messages stratégiques des Gardiens sont conçus pour défier leurs adversaires, tromper leurs forces armées sur les capacités militaires de l'Iran, les dissuader d'intervenir militairement et les convaincre de la robustesse du régime[24].

Ce système d'influence est prolongé sur le plan régional par l'intermédiaire de la Force Quds dont la fonction est de cultiver les liens avec les organisations chiites et pro-iraniennes comme le Hezbollah libanais. Dans le contexte libanais, cela inclut la diffusion de messages pro-régime à travers le réseau des mosquées et des *husseiniyyas* (lieux de congrégation religieuse) autant que *via* les médias rattachés à l'IRIB[25]. À son tour, le Hezbollah agit en médiateur (*proxy*) de la stratégie d'influence iranienne en relayant le message iranien au sein de la société libanaise[26]. La meilleure illustration est offerte par la guerre dite des 33 jours de l'été 2006 au cours de laquelle le Hezbollah a permis à l'Iran de remporter une victoire symbolique sur Israël en s'appuyant sur Al-Manar (Le Minaret), sa chaîne satellite. « Le Hezbollah ce n'est pas seulement des missiles et des combats, sinon le peuple nous aurait abandonnés depuis longtemps », déclarait alors Ghassan Darwish, l'une des têtes pensantes de la milice libanaise[27]. Au terme de ce qui restera comme l'une des premières info-guerres du XXI^{e} siècle, l'Iran et ses alliés régionaux ont réussi à acquérir une place prépondérante sur l'échiquier régional et à s'affirmer comme les leaders du « front du refus » anti-israélien, anti-saoudien et anti-occidental[28].

Une diplomatie publique sophistiquée et hybride

La diplomatie publique iranienne a su coévoluer avec l'approche asymétrique de la République islamique pour devenir un système d'influence sophistiqué comparable dans sa conception et dans sa conduite avec ceux de la Chine et de la Russie. Initialement centralisée, elle a pris le tournant du modèle bureaucratico-entrepreneurial qui consiste à minimiser l'action gouvernementale et à recourir le plus possible à des partenaires privés ou étrangers[29]. L'objectif est de légitimer la politique internationale du régime islamique et de présenter l'Iran sous son meilleur jour. Ce faisant, le slogan (*shoar*) est de « démontrer au monde que le pays est à la fois ouvert et tolérant[30] » ou, alternativement, de lutter contre ce que les autorités iraniennes appellent l'iranophobie (en persan *Iran Harāssi*) imputée selon elles à la propagande adverse[31]. Au-delà, il s'agit de mettre en œuvre l'un des principes fondamentaux de la doctrine diplomatique de la République islamique : nouer de fructueuses relations politiques, économiques et militaires aux quatre coins du globe et s'imposer comme un acteur qui compte dans l'arène internationale.

L'IRIB comme chef d'orchestre

Renforçant la politique d'influence du Sepāh-e Pāsdārān, l'IRIB est la principale agence en charge de la coordination des différents organes de la diplomatie audiovisuelle iranienne. Avec un budget annuel d'un milliard de dollars, plus de 13 000 employés, des succursales dans 20 pays du monde, notamment en Allemagne, au Brésil, en Malaisie et aux États-Unis, l'IRIB est, avec le CGRI, l'autre chef d'orchestre de la stratégie d'influence iranienne[32]. Selon la section 175 de la Constitution islamique, l'IRIB est placée sous la surveillance du Chef du pouvoir judiciaire et de l'Assemblée consultative islamique et directement elle-même subordonnée à la volonté

du Guide suprême de la révolution à qui revient la nomination de son directeur exécutif. Comme indiqué sur le site Internet de la branche française, ses initiatives « visent à informer le public étranger […] afin de promouvoir l'histoire et la culture iraniennes auprès de toute personne souhaitant avoir une compréhension réaliste de [l'Iran], dont la riche civilisation s'étend sur des millénaires[33] ». À cette fin, le service est utilisé pour diffuser les valeurs du régime et défendre « la position officielle du gouvernement de la République islamique d'Iran sur les grandes questions internationales[34] ».

Le système de diplomatie audiovisuelle iranien est complété par toute une série d'autres institutions publiques. Pour le contenu culturel, l'IRIB s'appuie sur le ministère de la Culture et de l'Orientation islamique et, en particulier, sur l'Organisation pour la culture et les relations islamiques (OCRI), l'organisation *de facto* pour la diplomatie culturelle de l'IRIB. L'OCRI a pour but de promouvoir « les liens culturels avec d'autres nations et communautés ; la consolidation des liens culturels de la République islamique d'Iran avec d'autres nations ; [offrir] une présentation adéquate de la culture et de la civilisation iraniennes ; préparer les bases de l'unité entre les musulmans ; la renaissance et la promotion de la culture et des enseignements islamiques dans le monde ; et la diffusion d'informations sur les principes et les réalités de la révolution islamique[35] ».

Pour le contenu informationnel, l'IRIB s'appuie principalement sur l'agence de presse IRNA (Islamic Republic News Agency) elle-même financée et contrôlée par le gouvernement et placée sous l'autorité du ministère iranien de la Culture et de l'Orientation islamique, qui, outre ses 60 bureaux iraniens, exploite 30 autres succursales dans divers pays du monde. L'idée est de maximiser le *soft power* iranien en multipliant les canaux et les langues à travers lesquels le message du régime est véhiculé dans le monde[36]. Il convient de noter que cette agence de presse officielle, déjà subordonnée par la loi au pouvoir exécutif, a vu sa sujétion au régime

renforcée depuis le début des années 2000[37]. Enfin, pour la dimension technique, la diplomatie audiovisuelle bénéficie de l'appui du ministère des Technologies de l'information et de la communication, principal organisme responsable de la gestion des systèmes informatiques et de communication de la République islamique.

À ce dispositif d'influence audiovisuelle il faut ajouter le ministère des Renseignements et de la Sécurité nationale, le VEVAK (acronyme de Vezārat-e Ettelā'at va Amniat-e Keshvar)[38] dont la contribution discrète mais cruciale consiste à assister l'IRIB en matière de propagande et de désinformation à travers la production de films documentaires faisant l'apologie du régime et de ses alliés ou, inversement, dénigrant les actions de ses adversaires régionaux et extrarégionaux[39].

Les grands médias audiovisuels et leurs publics cibles

Outre les douze chaînes de télévision nationales et les trente chaînes de télévision provinciales, l'IRIB supervise quatre chaînes de télévision d'informations internationales, six chaînes de télévision par satellite destinées aux téléspectateurs internationaux et trente grandes stations de radio. La diffusion se fait par ondes courtes et par satellites[40] en plus de 30 langues dont l'albanais, l'allemand, l'anglais, l'arabe, l'azéri, le bosniaque, le kurde, l'espagnol, le français, l'hébreu, l'italien et le russe – un vaste éventail linguistique qui atteste des ambitions globales de l'Iran mais aussi des cibles de sa politique étrangère. En plus des programmes d'information, l'IRIB produit chaque année 5 000 heures d'émissions de télévision, 300 films et 20 000 minutes de films d'animation[41]. Les fers de lance de ce dispositif de diplomatie audiovisuelle sont Press-TV, Al-Alam, Jamejam, Al-Kawthar TV, Voice of the Islamic Republic, Sahar Network et Hispan-TV. Les trois exemples suivants montrent que chacune d'entre elles est pensée pour cibler un public spécifique.

Lancée lors de l'invasion américaine de l'Irak, la chaîne satellite Al-Alam (Le Monde, en arabe) s'adresse essentiellement à un public irakien, chiite et arabophone. Avec des bureaux à Téhéran, Bagdad et Beyrouth et pouvant être visionnée sur tout le territoire irakien sans récepteur satellite, cette chaîne d'information propose également des émissions sur les affaires, le sport et la culture. Elle a pour vocation d'offrir une alternative aux autres chaînes satellites opérées par les monarchies du Golfe tout en véhiculant auprès de la population arabe une image favorable de la République islamique. Sa couverture de la guerre des 33 jours de l'été 2006 a notamment mis l'accent sur l'aide humanitaire iranienne au profit de la reconstruction du Liban afin de susciter une vague de sympathie à l'égard du régime islamique. « Ces images, note Saeid Golkar, ont été bien accueillies par les nombreux musulmans arabes qui avaient eu à souffrir d'un sentiment d'humiliation sous la domination coloniale[42]. » Ce type d'opérations médiatiques aurait, selon certains rapports, permis à la chaîne iranienne d'augmenter l'aura du régime iranien en Irak et dans les pays de la région[43].

L'autre chaîne satellite iranienne, Press-TV, est inaugurée en 2007 dans l'espoir de concurrencer les autres plateformes d'information continue comme la BBC World News, RT, DD India, CNN, France 24, Al-Jazira ou encore Deutsche Welle. Dès son lancement, les autorités iraniennes affichent cette volonté : « Le gouvernement souhaite utiliser Press-TV pour contrer ce qu'il considère comme un courant constant de propagande occidentale contre l'Iran, ainsi que pour offrir une vision alternative de l'actualité mondiale[44]. » Disposant d'un budget annuel de 25 millions de dollars, cette chaîne d'information en continu cible un public occidental et diffuse en anglais aussi bien qu'en français. Bien qu'elle soit, elle aussi, destinée à soigner la réputation internationale de l'Iran, Press-TV illustre à quel point, loin d'être coulée dans le même moule, chacune de ces chaînes est soigneusement conçue et opérée en fonction du public auquel elle

s’adresse. Alors que les présentatrices d’Al-Alam portent leur hijab (*tchador*) au plus près du modèle arabe, sur Press-TV, elles l’arborent de manière plus libérale tout en portant du maquillage et des tenues plus colorées ; autant d’éléments prohibés sur les chaînes de télévision nationales iraniennes. Ces efforts n’ont pas empêché Press-TV de se voir accuser de servir la propagande du régime islamique et de voir sa licence révoquée dans plusieurs pays européens et asiatiques au cours des années 2010[45]. Les autorités américaines ont même envisagé de classer le média iranien comme une « entité terroriste ».

En plus de soigner l’image de l’Iran comme champion de la résistance islamique face aux pays occidentaux, la diplomatie audiovisuelle cultive sa réputation de puissance anti-impérialiste auprès de pays non musulmans, autrefois non alignés, comme ceux d’Amérique latine et d’Afrique subsaharienne[46]. C’est dans cette optique qu’est lancée, en décembre 2013, Hispan-TV, la chaîne satellite hispanophone de l’IRIB[47]. Appuyée par la rédaction « Moyen-Orient » de la chaîne d’information en anglais de Press-TV, Hispan-TV bénéficie, en outre, lors de son inauguration, d’un partenariat stratégique avec la rédaction de la chaîne télévisée néo-bolivarienne Telesur. Procédant de la stratégie de défense avancée de l’Iran, cette percée médiatique en Amérique latine vise à s’adresser directement aux peuples latino-américains et à s’implanter durablement dans l’arrière-cour des États-Unis[48].

Nouveaux médias et réseaux privés

En marge de ces grandes plateformes de communication, la diplomatie audiovisuelle iranienne se démarque de ses rivales régionales en s’appuyant sur une centaine de médias semi-officiels et non officiels lui permettant de « privatiser » son action et d’adapter son discours à des publics spécifiques[49]. Ainsi, au Bahreïn, elle cible la population chiite par

l'intermédiaire de la radio Voice of the Republic et de la chaîne satellite Al-Sahar. La télévision et la radio Ahlulbayt, soutenues par l'Iran, couvrent le sud de l'Irak avec une programmation religieuse. La télévision Tamadon (« Civilisation ») diffusée à Kaboul permet d'atteindre les élites afghanes à l'aide d'un réseau de diffusion et de relais dans lequel le régime iranien a lourdement investi[50]. Appliquant le modèle bureaucratico-entrepreneurial, les stratèges iraniens recourent aussi régulièrement à des médias non iraniens. Cette stratégie de « blanchiment de l'influence » iranienne a notamment été appliquée en Afghanistan à travers des initiatives appuyées par un budget annuel de 100 millions de dollars comme la création d'un « syndicat de journalistes locaux[51] ».

Par ailleurs, la République islamique a très vite compris l'enjeu d'influence que représente Internet. Tissant sa propre toile sur le World Wide Web, l'Iran exploite activement les réseaux sociaux comme Twitter et Facebook pour étendre son entreprise de conquête des esprits à une audience sans précédent[52]. Pionnière dans ce domaine, l'Agence de presse de la République islamique, l'IRNA, a été l'une des premières à contribuer à l'e-diplomatie iranienne. Elle a rapidement été suivie par des journaux proches des milieux conservateurs, tels que *Kayhān* et *Iran*[53]. Dans le but d'augmenter son audience et de cultiver sa réputation de média impartial, Al-Alam lance en 2007 un site Web en anglais, puis une version en arabe et en persan. Avec son site en persan, en anglais, en arabe et en turc, Fars News, une autre agence de presse gouvernementale liée aux Gardiens, est l'un des principaux supports de la propagande du régime iranien sur Internet. Entre autres sites contrôlés par le gouvernement iranien, citons également Iran Didbān (observatoire) (www.irandidban.com) disponible en persan, anglais et français, ainsi que Habilian Foundation (www.habilian.ir) affilié au VEVAK et notamment disponible en arabe, en anglais et en persan[54].

Avec plus de 700 000 blogs en persan, qui figure parmi les 10 langues les plus parlées dans ce domaine, la blogosphère s'est vite imposée comme un enjeu majeur de la diplomatie publique iranienne. Le Guide suprême de l'Iran, l'ayatollah Khamenei, l'actuel président Hassan Rohāni ainsi que ses prédécesseurs, Mohammad Khatami ou Mahmoud Ahmadinejād, ont utilisé leurs propres sites comme autant de plateformes pour diffuser les positions officielles et l'idéologie de la République islamique. Il faut ajouter que les populations persophones résidant hors Iran en Afghanistan, au Tadjikistan, à Bahreïn, à Oman, dans les émirats ou encore en Californie, auxquelles s'ajoutent celles qui parlent le kurde, le tadjik ou le dari (appartenant à la famille des langues iraniennes) constituent un bassin naturel pour la diplomatie audiovisuelle et Internet de l'Iran.

Comme dans les médias traditionnels, le régime iranien privilégie une approche qui combine la supervision bureaucratique et l'action entrepreneuriale en utilisant des intermédiaires non officiels, privés et/ou étrangers[55]. Cette approche hybride est loin de se limiter au monde arabo-musulman. Fin 2018, les Iraniens sont accusés d'utiliser des milliers de faux comptes privés sur des médias sociaux comme Facebook pour conduire une vaste campagne de désinformation à l'échelle planétaire[56]. Les Gardiens de la révolution, dont la branche cyber est considérée comme la quatrième en son genre, sont régulièrement soupçonnés de recruter des services de cyber-mercenaires étrangers pour conduire des opérations de piratage mais aussi d'influence et d'ingérence politique[57]. Ce mélange des genres implique également la collaboration avec d'autres gouvernements. Il est assez symptomatique que Washington se soit régulièrement inquiété ces dernières années que Téhéran coordonne ses activités d'influence avec Pékin et Moscou pour influencer la politique interne des États-Unis[58].

À travers ses différents canaux et ses différentes initiatives, le régime iranien s'efforce de ternir la réputation de ses adversaires tout en présentant une image alternative de l'Iran, celle d'une nation islamique indépendante

et démocratique opposée aux États-Unis et à leurs alliés au Moyen-Orient[59]. En dépit des fluctuations de forme et de style, ce message est martelé de manière constante et cohérente faisant dire à Michael Rubin que la diplomatie audiovisuelle iranienne « ne souffre d'aucune confusion éditoriale[60] » et attestant de la remarquable cohérence de la diplomatie publique iranienne avec le reste de sa stratégie asymétrique.

*

Le choix de la stratégie asymétrique par l'Iran est donc à la fois le fruit de sa culture stratégique, elle-même modelée par les ingérences qui ont ponctué son histoire plurimillénaire, de sa situation d'enclavement géopolitique et de la lecture pragmatique que font ses dirigeants de la configuration de puissance de ce début de XXIe siècle. Dans ce contexte caractérisé par la suprématie encore incontestable des États-Unis et de ses alliés régionaux et extrarégionaux, la République islamique sait qu'elle ne peut espérer promouvoir ses intérêts à travers la confrontation directe avec ses adversaires. À l'instar de la Chine et de la Russie, elle pense néanmoins y parvenir à travers une approche alternative consistant à compenser ses faiblesses relatives dans les domaines traditionnels de la puissance par l'utilisation d'un certain nombre de moyens indirects parmi lesquels l'information, la désinformation, la subversion et la diplomatie de masse.

Dans ce contexte hypermédia où les combats se gagnent autant sur le front des opinions publiques que sur les champs de bataille conventionnels, l'Iran a su puiser dans la multitude d'outils d'influence mise à sa disposition par la révolution de l'information pour développer une diplomatie publique sophistiquée passant par les canaux d'information officiels mais aussi, et de plus en plus, par l'entremise de porte-parole privés et étrangers. Une stratégie d'influence hybride, déléguée et délocalisée permettant d'accroître l'espérance de vie du régime et de poursuivre sa stratégie de défense avancée (*forward defense*) tout en restant

sous le seuil de la conflictualité directe. Cette politique tous azimuts, conduite sur tous les fronts et par tous les moyens disponibles, risque de constituer un défi important pour les pays occidentaux surtout si, comme le pensent certains experts, elle est coordonnée avec celle de Pékin et de Moscou[61].

Pour aller plus loin

ALIKHAH Fardin, « A brief history of the development of satellite channels in Iran », *Global Media and Communication*, 2018, vol. 14, n° 1, p. 3-29.

BEHRAVESH Maysam, « Press TV : Iran's revisionist voice in perspective », *Asian Politics & Policy*, 2013, vol. 5, n° 4, p. 683-686.

BLOUT Emily, « Iran's Soft war with the West : History, myth, and nationalism in the new communications age », *SAIS Review of International Affairs*, 2015, vol. 35, n° 2, p. 33-44.

DAI Hassan, « Middle Eastern interventions in Africa : Tehran's extensive soft power », *Middle East Quarterly*, automne 2018, vol. 25, n° 4.

DUNCOMBE Constance, « Twitter and transformative diplomacy : Social media and Iran-US relations », *International Affairs*, 2017, vol. 93, n° 3, p. 545-562.

GOLKAR Saeid, *The Islamic Republic's Art of Survival : Neutralizing Domestic and Foreign Threats*, Washington Institute for Near East Policy, Policy Focus #125, juin 2013.

HONIG O. A. et YAHEL Ido, « The art of subversive conquest : How states take over sovereign territories without using military force », *Comparative Strategy*, 2017, vol. 36, n° 4, p. 293-308.

HUSSAIN Muzammil M., « The state of digital exception : Censorship and dissent in post-revolutionary Iran », in *State Power 2.0.*, Abingdon, Routledge, 2016, p. 47-58.

KAMAL Abdol Moghset Bani, « Evaluating the Islamic Republic of Iran's public diplomacy », *Uluslararası Politik Araştırmalar Dergisi*, 2018, vol. 4, n° 2, p. 22-39.

KARGAR Simin et RAUCHFLEISCH Adrian, « State-aligned trolling in Iran and the double-edged affordances of Instagram », *New Media & Society*, 2019, vol. 21, n° 7, p. 1506-1527.

MOWLANA Hamid, *Triumph of the Image : The Media's War in the Persian Gulf, a Global Perspective*, New York, Routledge, 2018.

PAHLAVI Pierre, « Understanding Iran's media diplomacy », *Israel Journal of Foreign Affairs*, 2012, vol. VI, n° 2, p. 21-33.

POSCH Walter, « Ideology and strategy in the Middle East : The case of Iran », *Survival*, 2017, vol. 59, n° 5, p. 69-98.

RUBIN Michael, « Strategies underlying Iranian soft power », *American Enterprise Institute*, mars 2017.

SREBERNY Annabelle et TORFEH Massoumeh, *Persian Service : The BBC and British Interests in Iran*, Londres, I.B. Tauris, 2014.

CHAPITRE 8

Les monarchies du Golfe : les guerres de l'information dans la crise de juin 2017

Fatiha Dazi-Héni

Ce chapitre a pour ambition d'analyser l'origine et les conséquences de la crise du Golfe qui éclate le 5 juin 2017 entre le Qatar et un quartet d'États arabes, composé de l'Arabie saoudite, du Bahreïn, de la fédération des Émirats arabes unis[1] (EAU), et de l'Égypte. Elle résulte à la fois de l'évolution de l'outil informationnel et des reconfigurations géopolitiques : l'explosion des réseaux sociaux à la fin des années 2000 et le déclenchement des révoltes arabes dans les années 2010. Elle vient aussi de l'émergence d'une nouvelle génération de leaders dans le Golfe qui adoptent des stratégies informationnelles offensives en rupture avec la tradition. Son caractère inédit tient à l'opacité et à la personnalisation accrue de ces régimes monarchiques qui se livrent à des querelles d'ego, contribuant à sa dramatisation.

Cette crise oppose certes le Qatar à quatre autres États, mais c'est la rivalité entre les EAU et le Qatar qui est au centre de cet imbroglio conduisant à une guerre de l'information. Ces deux États sont aussi les seuls à avoir supprimé leur ministère de l'Information, le Qatar en 1996 et les

EAU en 2006. En 1996, Doha (la capitale du Qatar) introduit la première chaîne satellite arabe, Al-Jazeera, qui révolutionne les médias arabes. Une décennie plus tard, la fédération des EAU met en place une diplomatie publique destinée à promouvoir la libéralisation économique de l'émirat de Dubaï (capitale économique de la fédération). L'émirat d'Abu Dhabi (capitale politique de l'État fédéral des EAU) conçoit quant à lui, au cours des années 2010, un narratif destiné à convaincre l'administration américaine qu'il est le meilleur rempart face au terrorisme islamique au Moyen-Orient.

Ces États autoritaires sont d'un type très différent de ceux étudiés dans le cadre de cet ouvrage, la Chine, la Russie ou même l'État totalitaire nord-coréen. Du fait de leur spécificité politique, il est nécessaire d'apporter un éclairage particulier sur ces régimes monarchiques néopatriarcaux avant d'analyser les stratégies informationnelles et d'influence mises en œuvre par les EAU et le Qatar.

Les ressorts de la crise du 5 juin 2017

La controverse entre le Qatar et les trois autres États membres du Conseil de coopération du Golfe (CCG)[2], à savoir l'Arabie saoudite, les EAU et Bahreïn, a plusieurs origines. Elle s'inscrit dans le prolongement d'une brouille diplomatique qui remonte à l'année 2013, au moment où le jeune émir Tamim du Qatar succède à son père, cheikh Hamad[3]. Elle est née de deux visions opposées de l'avenir du monde arabe lorsque les révoltes ont éclaté dans plusieurs pays de la région.

D'un côté, le Qatar a incité à s'adapter aux changements, en acceptant l'alternance politique consécutive aux soulèvements populaires, d'où son appui aux islamistes d'al-Nahda en Tunisie, mais aussi plus tard à Nida Tounis (parti sécullariste) ou encore à l'élection du président islamiste

égyptien, Mohammed Morsi. De l'autre, les trois États du Golfe ont soutenu l'ordre ancien et considéré qu'il fallait renforcer les appareils coercitifs en sécurisant les régimes en place, d'où leur appui au coup d'État militaire conduit par le maréchal égyptien Al-Sisi, qui, le 3 juillet 2013, a déposé le président Morsi. Cette crise sans précédent résulte en réalité de divergences de vue nées des soulèvements populaires arabes dans les années 2010 où des désaccords sur le rôle des Frères musulmans dans la région se sont transformés en une question sécuritaire fondamentale.

Lors de la mise en place du CCG en 1981, dans le but de se prémunir contre les menaces liées à l'émergence de la République islamique d'Iran en 1979, suivie un an après, de la guerre Iran-Irak, un consensus relatif existait autour de la menace iranienne. Certes, cette menace était diversement appréciée mais tout le monde s'accordait sur sa réalité. Les révoltes arabes rompent cet équilibre entre les pays du CCG : tandis que le Qatar soutient les Frères musulmans, Abu Dhabi et Riyad les rejettent. Ce contexte nouveau de tensions exacerbe les jeux d'influence et déclenche une guerre de l'information. Les EAU considèrent que l'islam politique constitue une menace structurelle qui divise les sociétés arabes et met en danger la sécurité nationale des États.

C'est ainsi que le 5 juin 2017, les États du quartet annoncent la rupture de leurs relations diplomatiques avec le Qatar et, plus surprenant, décident, le lendemain, d'imposer des sanctions inédites pour l'isoler en fermant leur espace aérien, maritime et terrestre. Cette décision abrupte met du jour au lendemain le Qatar devant le fait accompli et marque une rupture nette avec la gouvernance et la communication traditionnelles des États du Golfe.

Les effets de la personnalisation des régimes néopatriarcaux du Golfe

Les États du CCG sont de type néopatriarcal comme l'a théorisé Hisham Sharabi[4]. S'inspirant de la conception originale wébérienne de l'autorité d'un patriarche et de sa famille, Sharabi l'adapte à des régimes traditionnels qui ont introduit une bureaucratie moderne pour se doter d'un appareil d'État. Ce modèle est utile pour comprendre le fonctionnement des monarchies dynastiques du Golfe[5]. La construction rapide de ces États a été facilitée par l'exploitation de la rente pétrolière et/ou gazière. Le contrôle de la rente par les dynasties régnantes permet une redistribution de la richesse aux sujets. C'est encore sur ce socle que reposent le contrat social de ces États rentiers et la légitimité des familles régnantes, qui ont ainsi obtenu l'allégeance des chefs de tribus. Ils ont étendu cette légitimité au reste de la société[6] en développant un système clientéliste, caractérisé par l'octroi massif d'emplois dans le secteur public et par la redistribution de la richesse.

Au cours de la décennie 2010, la personnalisation des pouvoirs monarchiques dynastiques s'est généralisée dans les pays du Golfe (à l'exception du Koweït et du Bahreïn). À cela s'est ajouté un changement générationnel avec l'arrivée au pouvoir de nouveaux leaders ayant une culture politique différente. Un nouveau chapitre des relations interrégionales s'est ouvert. Les chefs d'État du Golfe privilégiaient une communication discrète lorsque des différends les opposaient afin de trouver une solution consensuelle. La révolution des réseaux sociaux permet à une nouvelle génération de dirigeants d'utiliser cet outil pour, notamment, inaugurer une guerre de l'information totalement étrangère à la culture locale.

La dynamique des réseaux sociaux dans l'environnement informationnel

Lors de la crise, les réseaux sociaux ont été les instruments d'une guerre de l'information destinée à saper la réputation du Qatar. Ils mêlent de façon outrancière, fausses informations et injures relayées par des comptes Twitter fictifs. La technologie est, avant même que la crise ouverte n'éclate, instrumentalisée comme arme de guerre informationnelle[7], lorsque, le 23 mai 2017, le site de l'agence de presse qatarie, Qatar National Agency et son compte Twitter sont la cible d'une cyberattaque[8]. Le contenu du communiqué du discours de l'émir qatari Tamim est dénaturé : il souligne à dessein l'excellence des relations avec l'Iran, le Hamas palestinien et le Hezbollah libanais – les pires ennemis de l'administration américaine et de ses alliés saoudien et émirati. Sans surprise, ce faux discours suscite l'indignation publique de ces derniers et leur sert de prétexte pour rompre leurs relations diplomatiques avec le Qatar, le 5 juin 2017.

Contrairement au président américain Donald Trump, les leaders du Golfe ne s'expriment pas directement sur leur compte Twitter pour faire passer des messages, *a fortiori* en période de crise. Les comptes des dirigeants servent, dans la continuité de la presse et des télévisions locales, à l'annonce de leurs agendas officiels. Les dirigeants préfèrent passer par de proches conseillers extérieurs à leur famille pour communiquer sur les réseaux sociaux. C'est cette stratégie indirecte que choisissent les dirigeants saoudiens et émiratis lors de la crise.

En Arabie saoudite, deux des principaux conseillers du prince héritier saoudien, Mohammed Bin Salman (MBS), sont à l'origine de la campagne de dénigrement anti-qatarie. Il s'agit de Turki Al Shaykh, président de l'Autorité des sports de mai 2016 à décembre 2018 et, depuis cette date, président de l'Autorité des divertissements, qui fait partie du cercle le plus intime du prince héritier[9], comme son acolyte, le sulfureux Saoud Al Qahtani, mis en cause dans l'assassinat du journaliste saoudien, Jamal Khashoggi, à Istanbul le 2 octobre 2018. Ces deux hommes de confiance, tous deux peu éduqués, sont issus des services de sécurité. Ils accèdent aux

plus hautes sphères du pouvoir de manière tout aussi fulgurante que le prince héritier, parachuté dauphin du trône, le 22 juin 2017 par son père, le roi Salman[10]. Al Qahtani a un rôle-clé dans la mise en œuvre de la campagne de diffamation dans la mesure où il agit au palais royal en qualité de directeur du centre d'études et des médias et de responsable de l'autorité cyber. Grand patron des plateformes des réseaux sociaux, il agit à l'aide d'une armée de soldats et de robots afin d'inonder les réseaux sociaux de tweets destinés à ternir la réputation du Qatar. Cette stratégie a également été utilisée en interne par les nouvelles autorités saoudiennes qui qualifient de traître toute personne susceptible de s'éloigner de l'orientation fixée par le prince héritier en matière de politique intérieure et extérieure.

Du côté des Émirats, la campagne menée contre le Qatar sur les réseaux sociaux est différente. C'est le ministre d'État des Affaires étrangères, le Dr Anouar Gargash, qui se charge de faire passer les messages officiels à destination du Qatar sur un ton tempéré. Ils sont cependant diffusés à outrance par des relais d'opinion comme certains chercheurs émiratis faisant autorité, le Dr Abdel-Khaleq Abdallah[11] ou la Dr Ibtisam al-Ketbi, directrice du Emirates Policy Center. Les EAU et l'Arabie saoudite semblent s'être partagé les rôles sans que l'on sache s'ils se sont concertés sur la question. Les EAU se montrent en revanche plus offensifs dans leur stratégie d'influence destinée à convaincre les cercles du pouvoir à Washington d'abandonner leur allié qatari.

Concernant le Qatar, les dirigeants choisissent, pour leur part, d'exprimer des messages souvent en réponse aux fausses informations par les voix du ministre des Affaires étrangères et de la porte-parole du ministère. En appui, la chaîne Al-Jazeera fait de la « communication stratégique », pour reprendre une terminologie empruntée à Joseph Nye[12], en diffusant des témoignages et des reportages sur les conséquences des sanctions adoptées par le quartet à l'encontre du Qatar[13]. La diffusion de ces documentaires commentés par des ONG humanitaires se fixe comme

objectif de montrer au monde que ses adversaires ne sont pas parvenus à l'isoler.

La guerre de l'information entre eux porte dès le début sur le champ sémantique utilisé pour définir la crise du Golfe, en arabe أزمة الخليج, sachant que les deux parties s'affrontent sur le qualificatif légitime. Le Qatar endosse le terme de blocus حصار tandis que le quartet reprend le terme anglais de *boycott*. La rivalité ne porte pas tant sur la validité juridique du terme que sur sa symbolique. De fait, le terme de blocus/حصار utilisé par le Qatar comporte une charge beaucoup plus forte dans l'imaginaire de la région car il renvoie au blocus de Gaza. Les Émiratis emploient aussi l'expression « isolement » du Qatar, عزالة ألقطرية, pour définir l'objectif à atteindre dans cette crise. Il est rapidement délégitimé car le Qatar démontre sa résilience en trouvant d'autres canaux d'approvisionnement et en développant des industries locales pour parvenir à l'autosuffisance.

La critique publique à l'encontre du Qatar tranche avec la tradition de ces pays dont les dirigeants ont toujours tenu à distance leurs ressortissants de toute prise de position en matière de politique étrangère. Cette remarque vaut particulièrement pour le cas saoudien où la diplomatie était synonyme de prudence jusqu'à la fin du règne du roi Abdallah, décédé en janvier 2015. Depuis l'arrivée du roi Salman et *a fortiori* de celle de son fils favori (MBS) comme héritier du trône en juin 2017, l'approche diplomatique privilégiée est le rapport de force[14]. C'est la preuve que la personnalisation accrue de ces pouvoirs a aggravé la tension, poussant les populations à prendre fait et cause pour leur leader qui incarne leur État respectif. Cette crise est l'occasion d'exprimer des rancœurs refoulées surgissant d'un passé mouvementé avec le voisin qatari. Ces dissensions datent de l'époque où cheikh Hamad, le père de l'actuel émir Tamim, a pris le pouvoir en déposant son père (très proche des Saoudiens et Émiratis) en

1995 et a instauré ensuite en 1996 Al-Jazeera qui a suscité la réprobation de ses voisins et celle de l'Égypte.

Des narratifs nationalistes exacerbés au cœur de la crise

La bataille virtuelle est exacerbée par une rhétorique ultra-nationaliste relativement nouvelle dans cette région, notamment en provenance d'Arabie saoudite où le nationalisme était déconsidéré en raison de l'orthodoxie wahhabite[15], seul référent identitaire permis. L'ensemble des pays du quartet (EAU et Arabie saoudite en tête) s'en empare pour jeter le discrédit sur le Qatar en l'accusant de conduire une politique hostile dans la région visant à mettre en danger la sécurité nationale de ses voisins. Ainsi, un ultimatum, adressé secrètement à Doha le 23 juin 2017, comprend 13 exigences qui portent largement atteinte à la souveraineté du Qatar. Parmi les mesures les plus intrusives auxquelles il est demandé au Qatar de répondre sous 10 jours, figurent la révision à la baisse de ses relations diplomatiques avec l'Iran, la fermeture de la base militaire turque et la fermeture de la chaîne de télévision Al-Jazeera.

Lorsque Doha transmet à CNN la liste, censée rester confidentielle, des 13 exigences formulées par le quartet, le hashtag « la liste est rejetée » devient viral sur Twitter. Le quartet, obligé de se rétracter, diffuse par le biais de la médiation koweïtienne une déclaration de 6 principes[16] moins contraignants, mais exigeant tout de même que le Qatar aligne sa diplomatie sur les accords de Riyad du 23 novembre 2013[17] et du 16 novembre 2014 portant sur la non-interférence dans les affaires intérieures des États voisins[18].

Pour répondre à l'ultimatum, Doha exacerbe à son tour la fibre nationaliste et fait de l'émir Tamim, le héros national qui a su défendre les intérêts du Qatar en résistant au « blocus » décrété contre lui. Le portrait

réalisé par un artiste qatari et intitulé تميم ألمجد (Tamim le Glorieux) devient viral sur les réseaux sociaux et sert même de blason dans le pays. Il est présenté comme une figure nationaliste intègre et victorieuse, aucun pays occidental et très peu d'États arabes ayant accepté de sacrifier leurs relations avec Doha. Ainsi, le Maroc et le Soudan, pourtant très proches de Riyad et d'Abu Dhabi, optent pour une position de neutralité.

En Arabie saoudite, Mohammed Bin Salman, le nouvel homme fort du royaume, organise une stratégie informationnelle articulée autour d'une rhétorique nationaliste portée par la *Vision 2030*[19], un programme destiné à diversifier l'économie du royaume. En réalité, cette vision est politique et recèle une propagande hypernationaliste[20] pour faire du royaume la nation arabe la plus puissante du XXIe siècle[21]. Celle-ci est au fondement de la réinvention d'un récit national, non plus fondé sur la religion, mais tourné sur l'histoire longue du royaume ; des sites antéislamiques sont réhabilités afin de promouvoir le tourisme et de valoriser l'archéologie par l'entremise d'un nouveau ministère de la Culture (mai 2016), jusque-là inexistant. L'outil digital est favorisé pour diffuser ce nouveau récit qui s'adresse à une population saoudienne dont la moyenne d'âge est de 27 ans, mais aussi au monde par le biais de campagnes publicitaires coûteuses. Les tensions dans la région, en particulier les crises avec le Qatar, l'Iran et la guerre au Yémen, servent aussi à exacerber, au sein de la population, un sentiment nationaliste. Néanmoins, la crise avec le Qatar reste largement incomprise en Arabie saoudite[22]. À l'opposé, la tension qui prévaut avec l'Iran et la guerre au Yémen suscitent une adhésion assez forte au discours sur la menace.

Les politiques sécuritaires des monarchies du Golfe n'obéissent pas aux principes structurant la plupart des États dans le monde, de type autoritaire ou démocratique, qui tous, sont dotés d'appareils institutionnels bien établis. Dans le cas précis du CCG, on observe une confusion entre la sécurité nationale et la sécurité des régimes car dans l'esprit des autocrates,

ces deux notions sont les deux facettes d'une même pièce de monnaie où le régime et l'État se confondent. Ce modèle est aujourd'hui poussé à son paroxysme avec la personnalisation de ces pouvoirs au fonctionnement opaque. Ainsi, les rivalités interétatiques se transforment en batailles d'ego.

Abu Dhabi versus Qatar : des stratégies informationnelles aux antipodes

L'émirat d'Abu Dhabi se heurte à une double difficulté pour mettre en place une stratégie informationnelle harmonieuse : d'une part, parler d'une seule voix au nom des sept émirats qui composent l'État fédéral ; d'autre part, s'inscrire dans le cadre d'une dynamique informationnelle collégiale *via* le quartet composé de pays qui comptent sur la scène internationale. Le Qatar fait face, seul. Toutefois, il bénéficie de la bienveillante médiation du Koweït et de la solidarité du sultanat d'Oman, ces deux États du Golfe ayant refusé de prendre part au conflit. Doha capitalise ainsi sur les difficultés d'Abu Dhabi à mettre en place une stratégie informationnelle unifiée et bénéficie de l'avantage de disposer d'une diplomatie publique plus aguerrie que celle portée par Abu Dhabi.

Selon Nicholas Cull[23], la diplomatie publique est le fruit de la communication d'un gouvernement à l'adresse d'un public étranger dans l'objectif d'exporter un narratif sur des sujets destinés à informer et/ou influencer un public extérieur. Elle s'appuie sur divers instruments allant des médias à l'organisation d'initiatives et d'événements publics et vise à tester et à formaliser des politiques gouvernementales et des narratifs auprès de publics extérieurs au pays. Partant de cette définition, le Qatar et Abu Dhabi optent pour deux stratégies bien distinctes. Avec Al-Jazeera, le Qatar

dispose d'un outil informationnel sophistiqué et très influent dans le monde, alors qu'Abu Dhabi est dépourvu d'un tel *soft power*.

Al-Jazeera, le coup d'avance de la diplomatie publique du Qatar

Al-Jazeera est le plus puissant relais d'opinion sur la scène arabe depuis la moitié des années 1990. Il a permis au Qatar, dépourvu des atouts de souveraineté et de puissance classique, d'inscrire sa marque de fabrique à l'échelle mondiale. Les retombées politiques et internationales sont immenses. La chaîne révolutionne un paysage médiatique arabe alors aseptisé et dominé par l'Arabie saoudite[24].

Le Qatar, sous la houlette des deux Hamad, l'émir Hamad et son comparse Hamad Bin Jassem (HBJ) ministre des Affaires étrangères et Premier ministre, fait, au milieu des années 1990[25], le choix d'une diplomatie publique, ouverte sur le monde, en rupture avec la puissance saoudienne qui exporte sa version salafiste de l'islam. Porté par son puissant *soft power*, le Qatar provoque l'ire des Saoudiens et de leurs voisins émiratis et bahreïnis en diffusant des débats politiques en présence d'opposants de tout bord (islamistes et progressistes sécularistes). Depuis, le Qatar est régulièrement accusé par ses voisins de semer la discorde par le biais de ce média. Al-Jazeera constitue la rupture culturelle la plus profonde dans la sphère informationnelle du monde arabe. Pour la première fois, un média arabe offre à la population une actualité articulée autour de débats contradictoires avec des spécialistes, des chercheurs, des opposants politiques, des activistes des droits de l'homme.

Cette chaîne n'est pas un organe d'État même si la manne gazière la finance largement. Conçue par une équipe de la BBC du service *Arab News*, elle a très vite émis des programmes en continu. Ce média a gagné en popularité dans l'ensemble du monde arabe et représente, à ce jour, le

succès le plus retentissant de la diplomatie publique qatarie. En 2010, le sondage annuel portant sur l'opinion publique arabe relève que pour 78 % des personnes sondées sur un échantillon de 10 000 personnes, Al-Jazeera constitue leur principale source d'information[26].

En 2006, le Qatar établit Al-Jazeera International, une chaîne en anglais destinée à un public occidental. Le professionnalisme et le ton percutant de cette chaîne permettent à un large public de se familiariser avec une vision arabe et critique de la région. La chaîne poursuit son extension en 2011 en émettant en langue turque, en swahili et en s'adressant également aux pays des Balkans. Ceci permet au Qatar de capitaliser sur sa stratégie informationnelle pendant la crise qui l'oppose au quartet et plus précisément aux EAU et à l'Arabie saoudite, d'autant que le groupe médiatique connaît un nouveau souffle lors des révoltes arabes. Le groupe est plus influent que jamais[27] avec sa chaîne de sport beIN, qui permet au Qatar d'être à la pointe en matière de diplomatie sportive et suscite la jalousie de ses voisins émiratis et saoudiens.

Doha procède aussi à une libéralisation économique audacieuse, rendue possible par ses immenses réserves gazières et le pari industriel du gaz liquéfié qui fera de lui le premier exportateur au monde au milieu des années 2000. Son PIB passe de 7 milliards de dollars en 1995 à 170 milliards en 2017. Cette aisance économique fait de lui l'État de la région le plus influent sur la scène arabe et mondiale et rend peu probable une contestation interne contre l'État-providence qatari. Par ailleurs, le Qatar abrite depuis 2003 deux bases militaires américaines parmi les plus importantes au Moyen-Orient : la base aérienne d'Al Udeid qui accueille 11 000 hommes et plus de 120 avions de combat, et la base d'Al-Salyha qui abrite le quartier général de l'US Central Command, à partir de laquelle sont conduites les opérations militaires d'Afghanistan, d'Irak et de Syrie. Le Qatar est devenu le pilier de la stratégie américaine au Moyen-Orient au grand dam d'Abu Dhabi.

Le Qatar est aussi le premier État du Golfe à rationaliser sa puissance financière au début des années 2000 : son fonds souverain, Qatar Investment Authority (QIA), permet de soutenir sa diplomatie de médiation tous azimuts et de financer des programmes de développement partout dans le monde (Afrique, Asie, Europe). Ce fonds souverain a subtilement servi à aider les États de l'OCDE à atténuer les effets de la grave crise financière mondiale de 2008.

L'affirmation de la diplomatie publique d'Abu Dhabi

Jusqu'à la fin des années 2000, le *soft power* de la fédération émiratie est essentiellement incarné par la vitrine libérale de l'émirat de Dubaï, ville-monde conçue par son émir, cheikh Mohammed Bin Rachid Al Maktoum. Il est à l'origine de l'adaptation du modèle de développement singapourien de Lee Kuan Yew qui a ensuite inspiré les autres États membres du CCG.

L'année 2006 est l'année pivot du changement radical de méthode de communication des EAU qui choisissent de dissoudre le ministère de l'Information et de le remplacer par le National Media Council (NMC). Après que le Dubaï World Port (DWP)[28] a essuyé, en cette année 2006, un échec retentissant en voulant acquérir six ports aux États-Unis, les dirigeants émiratis ont compris combien une campagne de désinformation pouvait être efficace pour façonner un discours et une décision politiques aux États-Unis. Une campagne bipartisane au Congrès a été menée pour s'opposer au contrôle d'installations portuaires stratégiques américaines par un État du Moyen-Orient situé dans une région largement stigmatisée par les attentats du 11 septembre 2001. En associant les EAU à un État soutenant le terrorisme, les décideurs politiques américains poussent les EAU à renoncer à leurs ambitions commerciales aux États-Unis.

Cet épisode incite les EAU à transformer leur appareil informationnel. L'objectif, dorénavant plus politique, consiste à exporter un narratif destiné

prioritairement aux États-Unis. Aux avant-postes, Abu Dhabi, capitale de l'État fédéral, élabore une stratégie informationnelle à plusieurs niveaux. Elle consiste d'abord à doter les EAU d'un *hard power* grâce à une armée bien équipée et entraînée ; ce processus a été initié dès les années 1990 par l'ancien chef d'état-major et actuel prince héritier d'Abu Dhabi, Mohammed Bin Zayed (MBZ). Il a plutôt réussi puisque le général James Mattis[29] a lui-même baptisé l'armée émiratie « Little Sparta ». Cet outil de défense sert à MBZ de faire-valoir pour exporter son narratif qui fait de son pays, doté d'une puissance financière avec ses riches fonds souverains (Abu Dhabi Investment Authority [ADIA] et Mubadala), un rempart contre l'islam politique et le terrorisme. L'autre dynamique d'influence choisie consiste à valoriser une diplomatie publique fondée sur l'identité de chacun des émirats qui composent la fédération.

Dubaï incarne surtout la diplomatie économique et de loisirs de la fédération et promeut Dubaï Expo 2020 : l'exposition universelle est l'événement phare de la région avant l'organisation de la Coupe du monde de football au Qatar en 2022. L'émirat de Sharjah (riche en gaz) développe une diplomatie culturelle conservatrice centrée sur la culture arabo-islamique du fait de sa proximité avec l'Arabie saoudite. Abu Dhabi mène davantage une diplomatie reposant sur des événements et des partenariats culturels mettant en relief des idéaux universels (Abu Dhabi Le Louvre, Sorbonne Abu Dhabi, Guggenheim Museum). Il promeut aussi des événements sportifs pour ne pas se laisser distancer par le Qatar qui a fait de la niche sportive son autre *soft power*. La quête universaliste de la diplomatie culturelle émiratie ambitionne de se caler sur le narratif séculariste diffusé à l'intention de l'Occident par le nouvel homme fort de l'État fédéral, MBZ.

L'émirat d'Abu Dhabi qui concentre 90 % des richesses pétrolières fédérales accroît son ascendant sur l'État fédéral, lorsque Dubaï est frappé de plein fouet par le krach financier mondial de 2008. Abu Dhabi prend

alors définitivement le contrôle de l'appareil informationnel et diplomatique de l'État fédéral et construit sa diplomatie publique sur un narratif sécullariste érigé en modèle du monde arabo-islamique. La personnalisation du pouvoir, autour du prince héritier, pourtant peu propice au sein d'une instance fédérale, devient une réalité lorsque le président de la fédération, cheikh Khalifa, est victime d'un accident cérébral, en janvier 2014.

L'ossature du processus décisionnel de l'émirat[30] s'organise alors autour du cercle rapproché du prince héritier, ses frères : Abdallah, ministre des Affaires étrangères, et Tahnoon, conseiller à la sécurité nationale, ou encore le général Issa Saif Al Mazrouei, vice-chef d'état-major et ancien directeur des renseignements internes (éminence grise du palais), et Ali Mohammed Al Shamsi, chef des renseignements extérieurs. L'appareil informationnel moderne d'Abu Dhabi organisé autour de technocrates, et plus précisément de trois figures-clés de la diplomatie émiratie depuis l'année 2008, agit sous le contrôle du noyau décisionnel articulé selon une conception ultra-sécuritaire du pouvoir.

Cependant, Abu Dhabi souffre d'un manque de culture communicationnelle et est très limité par des médias essentiellement arabophones[31], comme *Sky News Arabia*. Seul son quotidien *The National* est anglophone et il n'a que peu de résonance à l'international. Cette carence incite Dubaï à accueillir des médias comme la chaîne satellite saoudienne Al-Arabiya qui, à défaut de s'imposer comme concurrente d'Al-Jazeera, la prive du monopole.

Le Dr Anouar Al Gargash est chargé par son ministre de tutelle de la réorganisation du ministère des Affaires étrangères. L'autre homme-clé de la diplomatie conventionnelle est le Dr Sultan Al Jaber, qui dirige à la fois l'Académie diplomatique émiratie (ministère des Affaires étrangères), la compagnie pétrolière nationale ADNOC et le NMC qui contrôle tous les médias émiratis. Le fonds souverain Mubadala, qui finance la campagne

d’influence pendant la crise, est dirigé par un autre très proche conseiller de MBZ, Khaldoon Al Mubarak.

Des stratégies d’influence opposées pour gagner le soutien des États-Unis

Au cours de la crise, l’émirat d’Abu Dhabi consacre ses efforts à exporter et à tester son narratif de meilleur rempart contre l’islam politique notamment auprès des lobbies proches de l’administration américaine sous le président Obama et surtout sous celle du président Trump. Le président Obama étant favorable à un accord sur le nucléaire avec l’Iran et aux changements dans le monde arabe, il n’a pas permis aux EAU de faire valoir leur narratif, en dépit du fait que son secrétaire à la Défense, Robert Gates, s’y montrait réceptif. En revanche, le président Trump, peu familier de la complexité géopolitique au Moyen-Orient, est très vite séduit par l’approche émiratie, malgré les réserves exprimées par son ministre des Affaires étrangères, Rex Tillerson (2017-2018), familier de la région pour avoir dirigé ExxonMobil, et de son ministre de la Défense, James Mattis (2017-2018), fin connaisseur du Golfe. Influencer la décision américaine devient l’enjeu principal de la guerre de l’information lors du déclenchement de la crise. Dans cette perspective, les EAU louent les services de sociétés lobbyistes américaines. Le Qatar y répond par une stratégie radicalement différente.

Le lobbying combatif d’Abu Dhabi

Avec les septièmes réserves mondiales de pétrole, leur fonds souverain, ADIA, le plus important au monde en termes de gestion d’actifs

(850 milliards de dollars) et 27 milliards de dollars d'achat en équipements militaires aux États-Unis au cours des dix dernières années, les EAU sont devenus, en une décennie, selon nombre d'experts américains du Moyen-Orient, l'État arabe le plus influent à Washington[32]. Il n'est ainsi pas surprenant que les efforts émiratis menés pour influencer la politique américaine se soient concentrés autour de sociétés de communication représentant les intérêts militaires américains et proches de l'État d'Israël. Tous ont en commun de vouer aux gémonies l'islam politique et le régime iranien[33].

Traumatisés par l'épisode DWP en 2006, les EAU copient le modèle des campagnes d'influence menées par les États-Unis, qui consiste à financer des associations, des think tanks et à disposer d'experts pour orienter les débats. Yusuf Al Oteiba, l'ambassadeur en poste depuis 2008 et proche de MBZ, est plus que jamais la clé de voûte de la stratégie d'influence émiratie mise en place aux États-Unis lors de la crise. Il devient, à partir de la moitié des années 2010, l'ambassadeur le plus influent à Washington, selon une enquête rapportée dans le site *The Intercept*[34]. Il identifie les cercles néoconservateurs à Washington comme étant les plus réceptifs au nouveau narratif émirati. Al Oteiba se place du côté de ceux qui craignent de voir l'ancien ordre sécullariste autoritaire s'effondrer au profit de mouvements d'opposition dominés par l'islam politique. Pour maximiser ses chances d'influencer la décision politique au sein de l'administration américaine, Al Oteiba s'associe aux Saoudiens afin de financer des sociétés de communication et de relations publiques américaines très liées à Israël et au cercle rapproché du président Trump. Ses liens privilégiés de l'ambassadeur émirati avec Jared Kushner, gendre du président Trump, ont permis de persuader le président américain d'adopter le narratif émirati[35], inscrivant ainsi les Frères musulmans sur la liste des organisations terroristes en avril 2017[36].

Le Center for International Policy (CIP)[37] publie des données intéressantes sur les nombreuses actions de lobbying émiraties aux États-Unis. Ce rapport vient à la suite des enquêtes sur les interférences russes dans le processus électoral américain. Le CIP fait le constat qu'une industrie d'influence étrangère, estimée à plus d'un demi-milliard de dollars, est destinée à façonner la politique étrangère américaine, mais qu'elle reste largement inconnue du public. Les États du Golfe, notamment les EAU, le Qatar et l'Arabie saoudite, entrent dans cette catégorie. Le département américain de la Justice s'avère être une source essentielle pour mesurer les politiques d'influence des États du Golfe aux États-Unis car il contraint à déclarer les activités rémunérées pour lobbying, chaque activité faisant l'objet d'une fiche FARA (*Foreign Agent Registration Act*).

Ce rapport indique que pour l'année 2017, 20 firmes américaines ont dépensé 20 millions de dollars pour exercer des activités de lobbying agissant pour les intérêts émiratis. Toutes ne révèlent pas l'ensemble de leurs activités de lobbying. Les informations livrées par quatre d'entre elles, Hagir Elawad, Harbour Group, Akin Gump et DLA Piper, montrent qu'elles agissent soit pour le compte de l'ambassade des EAU aux États-Unis, soit pour l'Autorité des Affaires exécutives d'Abu Dhabi. Cet organisme chargé de conseiller la politique stratégique du prince héritier d'Abu Dhabi est dirigé par Khaldoon Al Mubarak qui gère aussi le fonds Mubadala.

Alors que les EAU ont surtout utilisé ces compagnies étrangères pour livrer leur narratif anti-qatari et expliquer les raisons de leur guerre au Yémen, ils leur confient le soin de cibler les individus, fondations et autres organisations susceptibles de relayer leur narratif. Cinq types d'organisation ont été la cible du travail de lobbying de ces sociétés : le Congrès, les organisations à but non lucratif, des médias, des think tanks et des universités. Au Congrès, ces sociétés se sont davantage efforcées de sensibiliser les personnels affectés aux comités des relations extérieures, du

renseignement, de la défense et des questions juridiques, que les élus. Ces quatre sociétés de lobbying ont également ciblé trois principales organisations à but non lucratif, la Smithsonian Institution, l'American Jewish Committee et l'United Way of Collier County. Des activités destinées à promouvoir les liens culturels et la collecte de fonds à la suite de catastrophes naturelles ou encore à resserrer les liens entre Israël et les EAU sur les questions de sécurité régionale, notamment liées à la menace iranienne, ont été privilégiées[38].

De même, c'est auprès de think tanks américains, tels que le CSIS, l'Atlantic Council, le Middle East Institute, le Hudson Institute, la Foundation For Defense of Democraties, l'American Enterprise Institute, le Center for American Progress ou la Brookings, que ces firmes ont agi pour promouvoir le narratif émirati. Al Oteiba a également forgé une relation étroite avec le Center New American Security (CNAS). Il s'agit de propager un narratif diabolisant le Qatar, justifiant la guerre au Yémen et présentant le leadership émirati comme l'allié arabe le plus fiable des États-Unis. Plusieurs conférences ont été consacrées à ces thématiques.

Les Émirats disposent d'autres vecteurs d'influence et de leaders d'opinion américains, tels George Nader, conseiller politique pour les Émirats, et Elliott Broidy, vice-trésorier du Comité national républicain[39]. Les EAU diffusent également leur influence dans les réseaux académiques en attribuant des donations à de grandes universités américaines connues pour abriter des programmes de recherche sur le Moyen-Orient comme George Washington, Johns-Hopkins, University of California, Los Angeles, New York University (NYU).

L'approche institutionnelle du Qatar

Face à la crise, le Qatar a quant à lui organisé une campagne institutionnelle didactique. Elle est essentiellement incarnée par le ministre

des Affaires étrangères, cheikh Mohammed Abderrahman Al Thani, sa porte-parole, Louloua Al Khater qui mobilise son équipe derrière le Government Communications Office (GCO), l'équivalent émirati du National Media Council. Al-Jazeera et la Qatar Foundation, créée par les parents de l'émir en 1995 et présidée par sa mère, cheikha Moza. Ce *hub* de l'économie de la connaissance possède un campus universitaire, Education City, qui abrite les antennes d'universités américaines réputées et qui a servi de tremplin aux autorités qataries pour organiser des discussions sur les tensions politiques dans la région.

Cette campagne a vocation à exposer, de manière factuelle, les conséquences de l'embargo subi par la population qatarie et les efforts déployés par le Qatar pour contourner les difficultés. Elle vise ensuite à rassurer ses grands partenaires commerciaux et stratégiques régionaux et internationaux, en contractualisant des accords de coopération et commerciaux très substantiels, notamment dans le domaine de l'armement.

Cette méthode d'influence a pour objectif de s'adresser directement aux États partenaires, puis d'avoir recours à des instances juridiques ou de régulation internationale pour contrer la campagne de dénigrement et de désinformation dont il est l'objet. Cette stratégie est à rebours de celle privilégiée par Abu Dhabi qui a exercé son action sur des acteurs non gouvernementaux susceptibles d'influencer les cercles politiques à Washington. Le Qatar assume au contraire une stratégie institutionnelle[40]. Le narratif qatari se structure autour de conférences données à Washington, mais aussi au sein de parlements européens, de think tanks basés à Londres, Bruxelles, Paris et Berlin. L'étendue des coopérations stratégiques étroites conclues de longue date avec les Occidentaux y est systématiquement exposée.

Le Qatar cherche aussi à conclure de nouveaux accords commerciaux pour consolider ses relations avec les acteurs internationaux les plus importants. Le président Trump change de ton sur la crise et exprime, dès le

11 juillet 2017, sa gratitude envers l'émir Tamim pour son soutien à l'Amérique dans sa lutte contre le terrorisme. Cette déclaration fait suite à la signature d'un contrat de 12 milliards de dollars pour l'achat d'avions de combat et la signature d'un accord bilatéral sur le contre-terrorisme. Le Qatar a également signé avec la France, en décembre 2017, un contrat d'armement pour l'acquisition de 12 avions Rafale en plus des 24 commandés en 2015. De son côté Londres, déjà bénéficiaire de contrats majeurs dans le secteur de l'armement et de l'immobilier, reçoit des garanties de soutien financier du Qatar Investment Authority qui s'engage à supporter les pertes que le Brexit occasionnerait. En somme, l'outil financier permet au Qatar de renforcer ses liens avec ses partenaires étatiques alors que les EAU s'en servent pour tenter de convaincre, par le biais de groupes privés, ses partenaires à lâcher le Qatar.

Le Qatar élargit sa stratégie étatique aux organismes internationaux : en juin 2018, il saisit la Cour internationale de Justice (CIJ), accusant les EAU d'atteinte aux droits humains dans le cadre de la politique discriminatoire à l'encontre des familles qataries. Le dossier qatari se fonde sur la Convention internationale sur l'élimination de toutes les formes de discrimination raciale de 1965, un des premiers accords internationaux sur les droits de l'homme, signé tant par Doha que par Abu Dabi. La CIJ, dont l'avis n'est pas contraignant, statue néanmoins en faveur du Qatar, en juillet 2018, ce qui permet à Doha de se présenter légitimement comme la victime de l'action du quartet. Ces discriminations sont étayées par les rapports d'ONG (Amnesty International, Human Rights Watch) qui ont pu les constater sur le terrain. D'autres organismes internationaux s'impliquent dans la crise à l'instar de la Fédération internationale de football association (FIFA), saisie par le Qatar en raison du piratage de sa chaîne de sport beIN par la chaîne saoudienne BoutQ[41].

Enfin, dans sa guerre digitale avec ses rivaux, le Qatar réagit dès le mois de juin 2017 en lançant une contre-offensive avec l'opération

GlobalLeaks[42]. Ce groupe de mercenaires hackers de la région du Golfe agissant pour le compte du Qatar a piraté les boîtes mail de l'ambassadeur émirati Yusuf Al Oteiba et d'acteurs américains engagés dans la campagne anti-qatarie, tel qu'Elliott Broidy. Le *New York Times* et le *Washington Post* ont diffusé au grand public les montants, acteurs et groupes de pression américains impliqués dans la crise. Les informations révélées par le CIP et relayées par ces grands quotidiens montrent au public américain le degré de l'influence exercée par les EAU pour modeler l'environnement informationnel sur la crise avec le Qatar[43] et peser sur la politique étrangère de l'administration américaine. Jusque-là, les Américains avaient conscience de ce type d'action en provenance de Moscou et non des pays du Golfe.

La guerre de l'information a baissé d'intensité depuis l'été 2019 en raison de l'exacerbation des tensions dans le golfe Persique entre Washington et Téhéran, plaçant les monarchies au centre du champ de bataille. Ce type de conflit hybride pourrait prendre une importance croissante dans le contexte géopolitique déjà complexe au Moyen-Orient. La guerre de l'information de la crise du Golfe pourrait se prolonger tant la bipolarisation entre les leaders du Golfe sur leur perception de la menace dans la région est vivace. Aujourd'hui, elle s'étend à d'autres théâtres, comme le conflit libyen, où les mêmes États s'affrontent : axe saoudo-émirati allié à l'Égypte versus axe turco-qatari. L'étude de la guerre de l'information qui oppose les monarchies du Golfe entre elles illustre la difficulté d'établir des normes pour réguler les dérives propres à ce type nouveau de crise. L'opacité et la personnalisation de ces régimes renforcent leur caractère discrétionnaire et autoritaire qui devient leur règle de fonctionnement. Dans ce contexte, ces États, membres d'instances multilatérales, devront jouer le jeu de la régulation internationale qui s'impose pour ces conflits hybrides. L'analyse de ces régimes patriarcaux permet de prendre en compte des dynamiques inexistantes dans d'autres

types d'États autoritaires. Elle s'avère utile pour évaluer le spectre des actions légitimes à mener dans le cadre de la mise en œuvre d'une régulation internationale applicable à tous les États.

Pour aller plus loin

CHAUVANCY François, *Blocus du Qatar : l'offensive manquée. Guerre de l'information, jeux d'influence, affrontement économique*, Paris, Hermann Éditions, 2018.

COATES ULRICHSEN Kristian, *Qatar and the Gulf Crisis*, Londres, Hurst & Company, 2020.

DAZI-HÉNI Fatiha, « La crise entre les pays du Golfe et ses impacts », *in* BENANTAR Abdennour, *Les Pays du Maghreb face à la crise entre les monarchies du Golfe*, Paris, L'Harmattan (à paraître).

KINNINMONT Jane, *The Gulf Divided. The Impact of the Qatar Crisis*, Middle East and North Africa Programme, Londres, Chatham House, mai 2019.

KRIEG Andreas (éd.), *Divided Gulf. The Anatomy of a Crisis*, Londres, Palgrave Macmillan, 2019.

III

LES DÉMOCRATIES FACE AUX GUERRES DE L'INFORMATION

CHAPITRE 9

Le Royaume-Uni : appréhender une sécurité réputationnelle[1]

Nicholas J. Cull [2]

La grande confusion médiatique entourant la crise ukrainienne de 2014 a surpris le gouvernement britannique. Londres s'est confrontée à la désinformation russe, ainsi qu'au refus de la Russie de reconnaître son rôle, avant de s'empresser de mettre au point une réponse efficace. La Première ministre Theresa May a formellement placé cette question en première ligne de la politique étrangère britannique le 17 novembre 2017, à l'occasion d'un discours très médiatisé qui l'a vue désigner la Russie comme un agresseur numérique cherchant « à transformer l'information en arme. Elle déploie les organisations médiatiques sous son contrôle pour implanter des histoires fausses et des images retouchées et ainsi essayer de semer la zizanie en Occident pour en fragiliser les institutions ». Sa réponse a été franche. Le Royaume-Uni a résisté et est demeuré fidèle à ses valeurs d'ouverture, expliquant « [qu'il] fera tout ce qui est nécessaire pour [se] protéger et travailler de concert avec ses alliés pour leur permettre d'en faire de même[3] ». Si les réponses en France, en Allemagne, au Danemark et

ailleurs ont été similaires, le cas britannique demande une étude plus précise. Tout d'abord, la Grande-Bretagne a une relation privilégiée avec les techniques de la guerre de l'information, ayant été pionnière en matière de tactiques, des meilleures comme des pires. Ensuite, la Grande-Bretagne était alors tout particulièrement vulnérable, faisant face à plusieurs crises simultanément : le Brexit, l'indépendantisme écossais et le retour de la question nord-irlandaise. Finalement, le Royaume-Uni offre un exemple de succès pour avoir mis au point une réponse globale au problème tout en faisant face à des incidents notables, tels que celui de Salisbury en mars 2018. Ce chapitre analyse l'émergence de la stratégie britannique et décrit certains de ses succès. Il montre qu'en 2019, le Royaume-Uni répondait aux problèmes liés à la désinformation tout en faisant de la liberté des médias dans les pays étrangers un élément important de son rôle international. Après avoir ainsi fait état des initiatives passées et présentes, nous clôturerons ce chapitre par une réflexion sur ce qui devrait être fait et par une série de recommandations pour renforcer la future réponse britannique à la transformation de l'information en arme.

La Grande-Bretagne et les débuts de la guerre de l'information

C'est la destinée d'un vieux pays à l'histoire si longue et si connue que d'avoir des exemples passés prêts à être rapportés à presque tout événement nouveau, qu'il soit positif ou négatif. C'est le cas de la guerre de l'information. Deux rois britanniques de la dynastie Stuart – Charles II et son frère Jacques II – ont cherché à restreindre la circulation de ce qu'ils appelaient des « informations fausses » (*false news*) à l'aide de proclamations royales signées respectivement en 1672 et 1688. Le

problème était alors interne au pays[4]. Mais, à d'autres moments, les intérêts officiels britanniques ont été entachés par des récits mensongers, lorsque les colons américains ont répandu des histoires atroces au début de la Révolution américaine, dans les années 1770, ou, en 1857, au moment de la révolte des cipayes en Inde[5]. Dans ce dernier cas, des rebelles ont raconté à des soldats musulmans au service de la Compagnie britannique des Indes orientales que les cartouches fournies pour les nouveaux fusils Enfield (qui ne pouvaient être ouvertes qu'avec les dents) étaient lubrifiées avec de la graisse de porc ; la même histoire – avec des cartouches lubrifiées à la graisse de bœuf dans leur cas – était par ailleurs racontée aux troupes hindoues[6]. Malgré toutes ces histoires dépeignant le Royaume-Uni en victime, le gouvernement britannique a appris, au cours du XX^{e} siècle, à faire de la communication un multiplicateur de son *hard power*, puis un substitut à ce *hard power* lorsqu'il a commencé à s'estomper aux quatre coins du monde.

Durant la Grande Guerre, le gouvernement britannique a beaucoup travaillé pour s'adapter aux canaux modernes de communication. De tous les gouvernements engagés dans le conflit, il a été le plus loin dans son utilisation des stratégies, les pires comme les meilleures. Parmi les pires, on retiendra par exemple la rediffusion de prétendues atrocités allemandes, comme la rumeur aujourd'hui célèbre de l'installation d'une usine de traitement des corps par les Allemands sur la crête de Vimy. Parmi les meilleures, on citera les pamphlets décrivant une alternative plus heureuse au monde de l'époque, fondée sur les droits et la technologie, commandés à H. G. Wells pour un lectorat allemand[7]. La portée des mots dans la victoire britannique demeure discutée mais il était dans l'air du temps d'en affirmer l'importance tout au long des années 1920. Aussi, durant l'entre-deux-guerres, plusieurs personnalités sont demeurées attachées au besoin d'une « projection nationale » efficace, pour reprendre les termes de l'époque. Pour le Royaume-Uni, le croque-mitaine a tour à tour été incarné par le

grand rival commercial américain, la « menace rouge » bolchevique, puis les dictateurs allemands, italiens et japonais. Les structures mises au point, ou préservées, par le gouvernement britannique du fait de cette angoisse se sont montrées utiles par la suite. On retrouve notamment le Bureau de l'information du Foreign Office (1914), les services extérieurs de la BBC (1932) et le British Council (1934)[8].

Durant la Seconde Guerre mondiale, la Grande-Bretagne a compris qu'il était important d'adopter une position morale élevée, tout particulièrement dans son approche des États-Unis demeurés neutres[9]. Le gouvernement a ainsi demandé aux services extérieurs de la BBC de prêter une attention particulière à l'exactitude de l'information diffusée, même lorsqu'elle était mauvaise. La Direction de la guerre politique (*Political Warfare Executive*) avait cependant pris conscience de la valeur de la contrefaçon et elle a cherché à tromper l'ennemi en secret avec de fausses stations de radio allemandes, des rumeurs orchestrées pour aggraver les divisions politiques internes, ainsi que des contenus écrits tels que des timbres affichant la tête d'Himmler au lieu de celle d'Hitler et qui ont été introduits dans le courrier allemand[10].

Après la Seconde Guerre mondiale, le gouvernement britannique a amélioré sa communication à l'intérieur du pays en créant le Bureau central de l'information (Central Office of Information, COI) et un Service d'information du gouvernement (Government Information Service, GIS) pour prodiguer et perpétuer cette nouvelle expertise technique à travers Whitehall (N.D.T. : le gouvernement britannique)[11]. Dans le reste du monde, le contexte de guerre froide a donné une plus grande importance aux médias libres et aux lignes éditoriales indépendantes, comme la BBC et le British Council par exemple. La BBC a réussi à défier le gouvernement Eden en donnant la parole aux deux camps opposés lors de la crise de Suez et en imposant à sa chaîne en russe (BBC Russian Service) d'éviter de critiquer directement les représentants du peuple russe – dont Staline – pour

se concentrer, à la place, sur les moments précis où la politique soviétique ne se montrait pas à la hauteur de ses promesses [12].

Cependant, malgré cette volonté affichée de favoriser une information équilibrée et ouverte, la Grande-Bretagne avait un « plan B ». De 1948 à 1977, le Foreign Office avait à sa disposition une unité secrète appelée le Bureau de recherche de renseignements (Information Research Department, IRD) qui était responsable de la création et de l'implantation des informations « utiles », au Royaume-Uni et à l'étranger, *via* des membres du Parlement, des journalistes, ou des experts prétendument indépendants. Les sujets liés à la guerre froide et à l'intégration européenne dominaient. Il y a même eu quelques incursions britanniques dans le domaine de la désinformation : une fausse station de radio égyptienne a été créée durant la crise de Suez par exemple. Des méthodes plus dures de guerre de l'information sont apparues durant les « urgences coloniales » du Royaume-Uni, sur des territoires tels que la Malaisie, le Kenya et Chypre [13]. Ces mêmes méthodes et leurs stratèges ont refait surface dans le nord de l'Irlande où l'IRD et les officiers de renseignement de l'armée britannique sont intervenus durant les années 1970 pour essayer de ternir l'image de l'adversaire interne que pouvait représenter l'IRA provisoire. Une rumeur de l'IRD liait l'IRA à des livraisons d'armes par sous-marins soviétiques, tandis que l'armée britannique murmurait que certains paramilitaires catholiques étaient secrètement satanistes, une idée « soutenue » par la « découverte » d'un autel impie couvert du sang de poulets sacrifiés. Dans une petite région où tout le monde se connaissait, de telles rumeurs ont été plus préjudiciables à ceux qui les propageaient qu'aux cibles visées [14].

Le gouvernement britannique a abordé les défis propres aux années 1980 fort de ces expériences passées. La Première ministre de l'époque, Margaret Thatcher, n'a jamais envisagé de trouver un compromis avec ceux qu'elle percevait – au Royaume-Uni ou à l'étranger – comme des ennemis. Cette approche agressive a été bien reçue par les publics d'Europe de l'Est.

Parmi les moments incontournables, on retiendra sa détermination à répondre en direct aux questions adressées par téléphone depuis les quatre coins du monde en octobre 1983, si bien que le technicien du service international de la BBC (BBC World Service) a été obligé de la couper pour respecter le temps imparti et clore l'émission. Ni l'événement ni sa conclusion n'étaient alors envisageables dans les pays du bloc de l'Est. L'agressivité de Margaret Thatcher envers les médias télévisés britanniques était particulièrement malvenue notamment lorsqu'elle les a accusés d'être des traîtres. Alors que l'époque encourageait à plus de transparence dans les médias, son gouvernement tenait à maintenir un certain contrôle au nom de la sécurité nationale. Pour reprendre les mots de son secrétaire de cabinet, Sir Robert Armstrong, alors qu'il défendait la censure face à un tribunal australien dans l'affaire Spycatcher en 1986 : le gouvernement se devait d'être « parcimonieux avec la vérité[15] ». Au même moment, l'armée britannique devenait plus à l'aise dans son approche des médias. La guerre des Falklands/Malouines de 1982 a démontré l'intérêt pratique d'un contrôle étroit de l'information en provenance d'une zone de guerre et du besoin de coopter les journalistes en offrant un accès privilégié à certains d'entre eux. Les États-Unis ont tiré des enseignements de ces pratiques quand ils ont révisé leurs doctrines lors des interventions sur l'île de Grenade, à Panama, et plus tard durant la première guerre du Golfe[16].

La Grande-Bretagne et les audiences étrangères

À la sortie de la guerre froide, le gouvernement britannique a pris conscience du besoin d'investir dans des moyens de communication efficaces. Dès 1992, le FCO a mis l'accent sur la vidéo en inaugurant sa propre chaîne de télévision par satellite : British Satellite News. Le gouvernement de Tony Blair a cherché à développer une approche

cohérente et sophistiquée des audiences étrangères en repensant la diplomatie publique britannique et en lui accordant des budgets plus importants. Le British Council a présenté son travail comme mutuellement bénéfique : l'organisation souhaitait « connecter l'avenir » des citoyens étrangers, entre eux et avec le Royaume-Uni. La BBC a, quant à elle, dévoilé un « plan Marshall des cerveaux » pour apporter son aide aux pays en transition post-communisme avec des programmes tels que le feuilleton télévisé en russe *Dom 7, Podyezd 4* (*7e maison, 4e entrée*). Tony Blair lui a donné sa bénédiction en y apparaissant comme invité vedette à l'automne 1997[17]. De son côté, l'armée britannique a continué à approfondir sa connaissance des opérations médiatiques ; lorsque le Royaume-Uni s'est engagé dans la campagne de l'OTAN en Serbie et au Kosovo, il a fourni la « grille » qui a donné une cohérence à la stratégie médiatique de toute l'alliance atlantique[18].

À la fin des années 1990, il était clair que l'approche gouvernementale de la communication devenait obsolète face aux progrès technologiques et à la réalité politique. Un audit mené par le Bureau du Cabinet en 1997, et présidé par Sir Robin Mountfield, a conduit à quelques changements dont la transformation du très respecté GIS en Service d'information et de communication du gouvernement. Mais de plus amples réformes étaient nécessaires. En quelques années, la capacité de l'entourage des élus, tel que le directeur de la communication de Tony Blair, Alistair Campbell, à utiliser les fonctionnaires pour communiquer sur des sujets politiques partisans a suscité l'inquiétude en Grande-Bretagne, au point de pousser les autorités à prendre des mesures à ce sujet. Cette inquiétude a atteint son paroxysme à la suite de la fuite d'un courrier électronique dans lequel Jo Moore, chargée de mission au ministère des Transports – et donc nommée par un élu – proposait à ses collègues de profiter du 11 septembre 2001 : c'était une « bonne journée » pour « enterrer » des « mauvaises nouvelles » qu'il aurait été nécessaire de dévoiler à un moment ou à un autre. Elle a par la suite

présenté ses excuses mais aurait recommandé une tactique similaire au moment de la mort de la sœur de la reine, la princesse Margaret, en février 2002. En 2002, l'audit Phillis (présidé par le PDG du groupe propriétaire du journal *The Guardian*, Sir Robert Phillis) a réduit la portée des pouvoirs des successeurs d'Alistair Campbell. Cet audit a mené à la création du Government Communications Network (GCN) qui a pris en main la numérisation des pratiques de communication du gouvernement britannique[19].

Le gouvernement de Tony Blair a pris au sérieux la notion de *soft power* et a cherché à promouvoir des représentations positives du Royaume-Uni à travers le monde. Cet effort a rapidement dépassé l'intérêt initial pour la promotion d'une image de marque nationale (*nation branding*) – à laquelle la presse britannique a donné le nom remarquable de *Cool Britannia* – dans le but de façonner une diplomatie publique cohérente. Un Conseil de diplomatie publique a été mis en place pour soutenir les canaux britanniques d'action publique à l'international – la BBC, le British Council, les ambassades, etc. – et promouvoir quatre objectifs stratégiques : contrer la radicalisation, assurer la sécurité climatique, soutenir la coopération avec l'Union européenne et promouvoir l'économie du savoir. Ce système a fait ses preuves[20]. Mais malgré ces investissements en soutien à la crédibilité britannique à l'étranger, le gouvernement de Tony Blair est resté associé, dans la mémoire de ses concitoyens, à la déformation de la vérité pour justifier l'intervention militaire en Irak. Une enquête publique de plusieurs années, pilotée par Sir John Chilcott, a depuis admis que le gouvernement avait exagéré le danger que représentaient les armes irakiennes de destruction massive et a conclu que la guerre « n'était pas nécessaire[21] ».

Depuis 2001, le gouvernement britannique a été particulièrement attentif au risque terroriste. En 2003, il a dévoilé une stratégie complète, nommée CONTEST en interne, qui inclut un volet PREVENT visant à

contrer la radicalisation au sein de la communauté musulmane britannique[22]. Cet effort pour déjouer l'islam radical en ligne et hors ligne a été coordonné par l'Unité de recherche, d'information et de communication (RICU) du ministère de l'Intérieur (Home Office), inaugurée en 2007. Ses méthodes couvrent un vaste champ, d'un soutien officiel à des blogs et à des comptes sur la plateforme de vidéos YouTube jusqu'à des moyens plus traditionnels tels que des dépliants d'information. Certaines activités de RICU n'ont pas été directement attribuées au gouvernement britannique et sont ainsi désignées, selon la nomenclature de la guerre psychologique au XX^{e} siècle, comme de la propagande grise. Le *Guardian* a critiqué ce manquement mais, à l'inverse des accusations portées contre RICU durant l'intervention irakienne, ces critiques n'ont pas trouvé un écho plus large[23].

Les interventions en Afghanistan – sous les couleurs de l'OTAN – et en Irak ont indiqué la prise en main des problématiques de communication par l'armée britannique. Le Royaume-Uni a contribué à la fois à la théorie et à la pratique de la guerre de contre-insurrection, insistant sur l'importance des « opérations fondées sur les effets » et sa donnée principale : les « dommages collatéraux » impliquant des civils durant une opération militaire sont toujours contre-productifs, quel que soit l'objectif ou l'intention initiale du commanditaire[24].

Comme souvent au Royaume-Uni, le passage de relais entre le gouvernement du New Labour et la coalition conservateurs/libéraux-démocrates de David Cameron n'a conduit ni à un changement de personnel, ni à un changement de politiques publiques dans les engagements internationaux du Royaume-Uni après 2010. Au contraire, le nouveau gouvernement a profité de projets lancés sous l'administration Blair tels que les Jeux olympiques de Londres en 2012, et de cadeaux de l'histoire comme le jubilé de diamant de la reine Elizabeth II, en 2012 également, le 800^{e} anniversaire de la Magna Carta (Grande Charte) en 2015, et le 400^{e} anniversaire de la mort de William Shakespeare en 2016.

Whitehall a préféré utiliser les termes de « communication stratégique » pour la couverture de ces événements. Si ce concept de « communication stratégique » était déjà bien connu des milieux d'affaires et des universitaires, cette utilisation nouvelle – synonyme de relations publiques – était une nouveauté pour le gouvernement ; d'ailleurs, en période d'« austérité », l'épithète « stratégique », avec ses connotations militaires, permet de justifier plus aisément un investissement financier que les termes de diplomatie publique[25]. Sous ce mandat, les structures de communication du gouvernement ont aussi été renforcées avec le lancement du Service de communication du gouvernement en 2013, une structure qui chapeaute tous les chargés de communication travaillant pour le Bureau du Cabinet[26]. La « Grande Campagne » demeure l'initiative de communication internationale phare du gouvernement Cameron. Elle a été lancée par le cabinet du Premier ministre en 2011, puis formellement en 2012, pour coordonner la communication internationale du gouvernement avec celles d'acteurs du secteur privé à travers un visuel stable et des qualités britanniques choisies, rappelant ainsi à une audience internationale que le patrimoine, la musique, l'innovation et le sport étaient des domaines éminemment britanniques[27].

Sous Cameron, la restructuration de l'armée britannique a conduit au développement des compétences en guerre psychologique et, par exemple, en janvier 2015, à la création très commentée de la 77e brigade, une nouvelle unité de spécialistes de la communication. L'armée avait prévu de recruter au-delà de 40 % de ses effectifs chez les réservistes, notamment parmi ceux qui possédaient déjà les compétences recherchées, numériques en particulier. Ces changements ont été interprétés de l'extérieur comme une volonté de préparer l'Angleterre au XXIe siècle, tout en faisant allusion à la guerre irrégulière d'autrefois : durant la Seconde Guerre mondiale, les soldats d'une autre 77e brigade, surnommés les « Chindits », s'étaient rendus célèbres en Birmanie[28].

Ce bilan historique mitigé de la communication gouvernementale britannique permet d'expliquer la complexité de la situation actuelle, dans laquelle des acteurs intérieurs et extérieurs répondent à des expériences tout à fait différentes. Pour les observateurs internationaux, ces expériences présentent le Royaume-Uni comme un partenaire de confiance dont les médias et les institutions gouvernementales sont perçues comme stables et crédibles[29]. Toutefois, la vie politique du pays a écorné cette réputation. Il ne sert à rien de chercher à l'étranger les voix critiques du rapport du gouvernement britannique à la vérité. Le sentiment de méfiance qui existe aujourd'hui à l'intérieur du pays a été utilisé efficacement par les adversaires stratégiques du Royaume-Uni.

L'avènement de la guerre numérique de l'information

Si la crainte d'une guerre de l'information a pris toute son ampleur en 2014, on retrouve des signes plus anciens de la vulnérabilité britannique. Durant la crise du Kosovo, en 1999-2000, plusieurs journaux ont fait état d'une curieuse initiative qui avait été lancée depuis le 10e étage du bâtiment le plus haut de Belgrade : un groupe de pirates informatiques y menait une campagne d'interférence numérique, appelée *YugoSpam* par la presse de l'époque. Cette équipe serbe ne s'est pas limitée à des attaques contre les sites Internet des gouvernements membres de l'OTAN ou des groupes de promotion des droits de l'homme, elle a également publié de la propagande nationaliste serbe sur les sites Internet anglophones qu'elle percevait comme culturellement emblématiques : Manchester United, James Bond, et un nouveau médicament pour la dysfonction érectile, le Viagra. C'était une ferme à trolls *avant la lettre*[30]. Au début du XXIe siècle, l'Angleterre –

comme les autres pays occidentaux – concentrait ses efforts sur Internet à lutter contre l'extrémisme islamique, reconnaissant ainsi que les technologies numériques avaient libéré un certain nombre d'activités transgressives de leurs contraintes géographiques. Le Quartier général de la communication (GCHQ) s'affairait à rechercher et à défaire les terroristes et les activités d'États hostiles, mais également à combattre le crime numérique sur le Dark Web. Ainsi l'initiative dévoilée en décembre 2014 par le GCHQ et dédiée à la pédophilie en ligne[31].

L'affolement de 2014 a également fait une grande place à la Russie, un problème qui était en germe depuis un certain temps. L'État russe a commencé à compliquer le travail des médias et des organisations non gouvernementales étrangères sur son territoire au début des années 2000. À partir de 2005, il a souhaité renforcer sa réputation à l'étranger, notamment face à l'hégémonie des chaînes BBC et CNN, grâce à une chaîne internationale de télévision : Russia Today. Il est devenu rapidement plus difficile pour le gouvernement britannique d'atteindre les citoyens russes. Puis, un contentieux fiscal fallacieux a mené à l'arrêt des activités du British Council en dehors de Moscou et à l'arrestation et à l'intimidation du directeur du bureau de Saint-Pétersbourg, Stephen Kinnock, à la fin de l'année 2007[32]. La guerre russo-géorgienne en Ossétie du Sud en 2008 s'est accompagnée d'un effort pour contrer la version occidentale des événements. L'année suivante, Russia Today est devenue RT et, d'une chaîne d'information sur la Russie, elle est devenue une chaîne d'information diffusant la vision russe du reste du monde. Cette nouvelle approche est parfaitement résumée par un slogan, adopté pour une campagne publicitaire en anglais en 2010 : *Question More*[33]. Puis, à partir de 2012, des nationalistes russes ont utilisé un arsenal d'outils numériques – dont des bots, trolls, mèmes, et une attaque généralisée contre la notion de vérité objective – pour noyer les voix d'opposition en Russie[34]. Le monde

n’a réellement pris conscience de ces événements que lorsque ces armes numériques ont été déployées à l’extérieur de la Russie.

La réponse britannique

La crise ukrainienne de 2014 a été un choc pour l’Occident, particulièrement pour son exposition médiatique. La communication était au cœur des activités russes durant le printemps 2014 : l’identité contestée des troupes présentes dans l’est de l’Ukraine, les revendications rivales sur le territoire de la Crimée, les sentiments supposés de la population de Crimée, l’identité des personnels mobilisés sur place, la guerre des mots après l’explosion du vol MH-17, le lancement du nouveau site d’information Sputnik – tous ces événements suggéraient que cet adversaire de l’Occident faisait usage de ses pouvoirs cinétiques et communicationnels. Les experts occidentaux de défense se sont retranchés derrière le concept de « guerre hybride » pour illustrer une stratégie apparemment nouvelle venant de Russie. Les Ukrainiens ont cependant répondu qu’ils vivaient cela comme une guerre traditionnelle[35].

L’OTAN a été pressée de trouver une réponse adéquate et ses membres se sont rapidement mis d’accord pour ne pas « combattre le feu par le feu ». Les pays de l’UE et de l’OTAN ont tous refusé de mener une campagne de désinformation, expliquant très souvent cette décision par ce refrain : « Cela ne nous ressemblerait pas[36]. » L’approche britannique se déclinait ainsi : premièrement, est-il nécessaire de répondre à la désinformation ? Deuxièmement, comment développer des médias indépendants dans les lieux les plus à risque d’une intervention russe et ainsi diminuer les chances d’un tel aventurisme ? Troisièmement, comment développer et renforcer les institutions de la société civile – au-delà des simples médias – pour rendre ces pays vraiment résilients face à une agression étrangère ? Le Fonds

européen pour la démocratie (FEDEM), qui a publié un rapport en juin 2015 proposant des mécanismes pour renforcer les médias indépendants auprès des populations russophones vivant hors de la Russie, se trouvait au nombre des partenaires de cette réflexion britannique. Le FEDEM recommandait par exemple de mettre en place un panier de fonds, une « usine à contenus » (*content factory*) et une nouvelle plateforme pour produire des contenus sérieux en langue russe[37]. Le Foreign Office s'est immédiatement engagé à soutenir plus efficacement les médias et la société civile des pays Baltes et de l'Ukraine en particulier. Les événements de début 2016 n'ont fait que redoubler les inquiétudes existantes. En janvier 2016, le faux viol de « Lisa F. » en Allemagne a montré que la Russie était capable et prête à s'attaquer à l'ordre social des pays d'Europe occidentale pour en accentuer les divisions internes à tout prix[38]. Cet épisode retentissant a montré distinctement le rôle des médias officiels russes aux côtés de la désinformation d'origine interne, au moment même où l'on allait retrouver cette alliance dans les votes-clés du référendum sur le Brexit et de l'élection présidentielle américaine.

Ce vote en faveur d'un départ de l'Union européenne est évidemment un défi pour la politique étrangère britannique mais, au niveau opérationnel, les unités responsables de la lutte contre la désinformation russe ont persévéré dans leurs efforts sans s'en inquiéter. Il était en effet nécessaire de montrer que le Royaume-Uni serait toujours un élément essentiel de l'avenir du continent européen – malgré le résultat du référendum – et que défaire l'influence du Kremlin demeurait dans son intérêt. Dès l'automne 2016, les premiers projets dans les pays Baltes et en Ukraine montraient des résultats positifs. La réponse du FCO se déclinait alors en « trois E » : révéler la désinformation lorsqu'elle était détectée (*expose*), renforcer les médias indépendants dans les espaces linguistiques vulnérables, notamment russophones (*enhance*), et collaborer avec les publics sous influence russe pour leur permettre de développer des institutions civiles fortes (*engage*)[39].

L'élément *expose* de cette stratégie soutient divers projets mettant en lumière la désinformation russe. Parmi les bénéficiaires de l'aide britannique, on retrouve StopFake.org, un site Internet de vérification de l'information basé à Kiev et créé par des étudiants et des enseignants de l'école de journalisme de Mohyla en mars 2014. Grâce au soutien de l'ambassade britannique à Kiev, de l'association londonienne Human Rights, du Sigrid Rausing Trust, et d'une série de petits donateurs, le site a pu s'agrandir et développer des plateformes en plusieurs langues européennes[40]. Le Service d'action extérieur de l'Union européenne a mené sa propre action en parallèle avec la création du programme *UE v. désinformation*[41]. Le FCO a financé l'Atlantic Council généreusement, et ce dernier abrite maintenant l'une des unités d'enquête sur la désinformation et la guerre numérique les plus reconnues : le Digital Forensic Lab[42]. Cet élément *expose* a ensuite été élargi pour proposer une aide aux « elfes » qui signalent la mésinformation et la désinformation en ligne et publient des corrections sur Twitter. Certains « elfes » travaillent toutefois sans l'aide du FCO ni de financements gouvernementaux. Parmi les plus connus, on note Bellingcat, un collectif d'enquêteurs en freelance fondé par le chercheur et « journaliste citoyen » britannique Eliot Higgins[43]. Au nombre des bénéficiaires de ces financements, on retrouve également une unité créée par l'organisation non gouvernementale écossaise Institute for Statecraft et baptisée Integrity Initiative. À sa création en 2015, la bannière Twitter de cette équipe arborait l'annonce programmatique : « défendre la démocratie contre la désinformation ». En dehors du FCO, elle a aussi reçu des fonds du département d'État américain et du ministère des Affaires étrangères lituanien[44].

L'élément *enhance* chapeaute plusieurs projets soutenant des médias indépendants. Au nombre des bénéficiaires, on retrouve une chaîne d'information en langue russe basée à Kiev, Hromadske TV, et la télévision publique estonienne, *via* des projets subventionnés par l'agence de

développement médiatique de la BBC, la BBC Media Action (anciennement appelée le World Service Trust)[45]. Le gouvernement britannique demeure un acteur important dans l'espace médiatique russophone grâce à ses subventions au BBC Russian Service et à d'autres chaînes en langues étrangères dédiées à des populations perçues comme vulnérables à l'influence russe. Ainsi, il n'est pas surprenant que la chaîne de la BBC en serbe ait repris du service en mars 2018[46].

Le travail du British Council pour promouvoir des initiatives en soutien à la société civile illustre l'élément *engage*. Parmi celles-ci, on remarque un programme du British Council appelé *Superheroes* en faveur de jeunes femmes entrepreneuses issues de plusieurs communautés estoniennes[47]. Le Good Governance Fund et les projets de la Westminster Foundation for Democracy soutiennent également la société civile. Cette dernière a notamment œuvré à professer l'alphabétisation médiatique dans des territoires particulièrement vulnérables. Le gouvernement britannique a finalement consacré ces projets en leur accordant le plus important appui qui soit : un budget en hausse. Soixante-dix millions de livres ont été affectés aux efforts médiatiques en langue russe pendant quatre ans[48].

Fin 2016, le gouvernement britannique a reconnu l'existence d'une crise. Début décembre 2016, le chef des services secrets britanniques, Alex Younger, a rompu avec le protocole et convié des journalistes au siège emblématique du MI6, à Vauxhall, et décrit cette concomitance d'activités hostiles de piratage, de propagande et de subversion comme une « menace fondamentale » pour les démocraties européennes. Il n'a pas nommé le pays à l'origine de ces attaques mais son choix d'utiliser les termes de « guerre hybride » a été suffisant pour pointer du doigt un acteur[49]. Onze mois plus tard, ce voile rhétorique n'était même plus à l'ordre du jour. Le 17 novembre 2017, la Première ministre Theresa May a formellement dénoncé la Russie comme la source de cette guerre de l'information[50]. À partir de ce moment, l'attention de Londres s'est portée sur l'étranger : la

confusion semée par les médias russes en Syrie, les machinations russes dans des pays tels que le Monténégro, où une tentative de coup d'État semblait avoir été soutenue par Moscou, ont fait l'objet de cette attention renouvelée. Mais la situation a changé en 2018 lorsque la guerre de l'information s'est aventurée sur le territoire britannique.

L'affaire Skripal et ses suites

Le 4 mars 2018, à 4 heures de l'après-midi, les urgences de la ville de Salisbury ont reçu un appel signalant deux personnes malades sur un banc du centre-ville. Quelques heures plus tard, le gouvernement britannique a annoncé qu'il s'agissait de l'ancien agent du GRU Serguei Skripal et de sa fille Ioulia, et qu'un agent neurotoxique datant de l'époque soviétique, le Novichok, était responsable de la détérioration de leur santé. Le Kremlin et des médias pro-Kremlin ont contesté la version des événements diffusée par le gouvernement britannique à l'aide d'une grande quantité de désinformation. La réponse britannique montre le degré de compréhension de la guerre de l'information acquise avec le temps et la facilité avec laquelle le gouvernement a retourné cet incident à son avantage. Le travail de lutte contre la désinformation, mené par les autorités américaines dans les années 1980, a montré qu'un cas de désinformation pouvait être utilisé pour discréditer le pays commanditaire. Les chargés de communication du FCO l'ont prouvé en profitant du fait que les médias russes et l'ambassade russe à Londres avaient successivement défendu 38 versions différentes de l'incident en pointant du doigt les États-Unis, le Royaume-Uni, l'Ukraine, une tentative de suicide ratée, puis une tentative de Ioulia Skripal – remarquablement bien armée dans ce cas – d'assassiner sa belle-mère[51]. Le nombre de « republications » de la ligne défendue par le FCO a été le signe de l'efficacité de sa stratégie, tout comme l'unanimité sans précédent de la

réponse diplomatique chez les alliés de la Grande-Bretagne (dont l'Union européenne et les États-Unis) qui ont expulsé 150 diplomates russes[52]. Les sondages successifs n'ont pas montré un intérêt particulier pour la version des événements portée par le Kremlin en dehors du monde russe[53].

Au plus haut de la crise de Salisbury, plusieurs enquêtes du gouvernement britannique se sont penchées sur le problème sous-jacent de la désinformation et de la propagande numérique. En mars, une nouvelle revue de sécurité nationale (*National Security Capability Review*) a dévoilé ce qu'elle a appelé la « doctrine Fusion » de la politique britannique de sécurité : celle-ci a souligné explicitement le besoin d'intégrer les outils de la communication, de la diplomatie, de la politique sociale et du *soft power* dans la politique étrangère britannique[54]. Comme l'expliquait alors Alex Aiken, directeur général de la communication du gouvernement : « [C]ela signifie que les communications stratégiques doivent être prises en compte avec le même sérieux que les options financières et militaires[55]. » Sa mise en place a conduit à l'inauguration en avril 2018 d'une Unité de réponse rapide (RRU) au sein de Whitehall[56].

Parallèlement à ces changements, une commission parlementaire *ad hoc* a enquêté sur la désinformation et la propagande numérique et a publié un rapport d'étape en juillet 2018. Si les menaces extérieures y occupaient une place importante, la commission a eu raison de se concentrer, dans le détail, sur les opérations numériques d'influence opérant depuis le Royaume-Uni, en prenant ainsi l'exemple de Cambridge Analytica et de son entreprise partenaire SCL Elections pour leur influence sur le vote du Brexit et lors d'élections aux quatre coins du globe. Au nombre des propositions, on retrouve plusieurs appels à adapter la législation existante et à proposer une loi électorale adaptée à l'ère numérique. Par-dessus tout, le rapport recommande d'arrêter d'utiliser les termes de *fake news*. Finalement, il souligne que des citoyens britanniques sont liés au problème[57].

La crise politique actuelle, provoquée par le Brexit, est le dernier élément de ce panorama. Si les diplomates britanniques ont redoublé d'efforts pour montrer que le Royaume-Uni reste un partenaire important dans les affaires internationales, des inquiétudes demeurent. Un désaccord sur les conditions du départ du Royaume-Uni de l'Union européenne a conduit à la démission du ministre des Affaires étrangères Boris Johnson en juillet 2018. À la surprise de tous, son successeur, Jeremy Hunt, s'est concentré sur les problématiques médiatiques. Il a très rapidement proposé une initiative majeure de diplomatie publique pour faire face à la crise médiatique que connaît le monde et ainsi défendre les médias indépendants. Au cœur de cette initiative, on trouve la Conférence mondiale sur la liberté des médias qui s'est tenue à Londres en juillet 2019 et a été co-présidée par Jeremy Hunt et son homologue canadienne Chrystia Freeland[58]. D'autres initiatives moins médiatisées ont vu le jour en 2019, dont la publication du manuel *RESIST : Counter Disinformation Toolkit* – rédigé par l'universitaire James Pamment et une équipe de l'université de Lund en Suède – qui détaille comment accroître les compétences de lutte contre la désinformation au sein du GCS[59]. En juillet, le Royaume-Uni a montré qu'il était prêt à adopter des sanctions sérieuses si nécessaire. L'Ofcom, l'autorité régulatrice des médias, a terminé son enquête sur RT et a condamné la chaîne à une amende de 200 000 livres en raison de « défaillances sérieuses » et d'un manque d'impartialité dans sa couverture de l'affaire Skripal. Si RT n'a pas perdu sa licence pour diffuser au Royaume-Uni, elle n'en est pas passée loin[60].

Dans cette bataille contre la désinformation, il est difficile de retenir des indicateurs de succès efficaces. Paradoxalement, tout indice qu'un effort de contre-propagande dérange l'adversaire a historiquement encouragé ces efforts. Pour le projet *Counter Disinformation and Media Development* du Foreign Office, ce signe est arrivé fin 2018 avec un piratage massif et la publication des documents volés à Integrity Initiative, une organisation

partenaire du FCO, par le groupe Anonymous. Les bloggeurs ont rapidement mêlé ces documents à un ensemble de thèses conspirationnistes, profitant ainsi de l'avènement de l'Expose Network, un mécanisme effrayant développé par la Grande-Bretagne pour contrer la désinformation[61]. Signe des difficultés de la politique informationnelle au XXIe siècle, les bloggeurs ont plus rapidement accepté l'interprétation des événements offerte par le Kremlin que celle du FCO. Un élément dévoilé, pourtant accessoire, a rapidement pris de l'ampleur : le compte Twitter d'Integrity Initiative a relayé des critiques du leader de l'opposition Jeremy Corbyn. En conséquence, le Foreign Office a été accusé d'être un vecteur de la propagande partisane au Royaume-Uni[62]. Le travail de cette organisation s'est pourtant poursuivi comme si de rien n'était.

Appréhender une sécurité réputationnelle

Après avoir détaillé la politique informationnelle globale du Royaume-Uni, il est nécessaire de s'attarder à décrire ce que cette politique pourrait idéalement devenir et les conséquences que l'on peut tirer de cette expérience britannique. La première conclusion que l'on peut en tirer est le besoin de corriger la notion de *soft power* définie par Joseph Nye. Depuis sa conception, elle a été perçue et utilisée par les hommes politiques britanniques, de Blair à Campbell, comme un luxe à disposition des pays les plus riches que l'on pouvait étendre en accumulant des succès aux Oscars ou en accueillant les Jeux olympiques. Mais le côté obscur de ce concept a fait son apparition depuis quelques années. En effet, la réputation est un élément fragile du pouvoir d'un État que des acteurs hostiles travaillent aujourd'hui pleinement à détruire. Si l'Ukraine était vue comme fragile en 2014, c'est en partie parce qu'il était difficile de définir ce que l'Ukraine « représentait » alors. Sa seule réputation était celle d'une république post-

soviétique paralysée par des difficultés internes. Les citoyens lambda d'Europe occidentale ne se sont pas particulièrement inquiétés de la perte des provinces ukrainiennes. L'Ukraine faisait face à une précarité réputationnelle. Et si l'on conçoit la réputation comme un élément notable de la sécurité d'un pays, répondre à la désinformation devient politiquement plus urgent et nécessaire. Les exemples récents de la « doctrine Fusion » et du projet *Counter Disinformation and Media Development* montrent que c'est déjà le cas au Royaume-Uni. La logique d'une sécurité réputationnelle induit le besoin de protéger l'intégrité des médias de masse à l'intérieur du pays mais également d'aider les autres pays à en faire de même. Finalement, ce concept incite à prendre conscience des vulnérabilités particulières soulignées plus haut dans ce chapitre[63].

Si les démocraties se concentrent souvent sur un seul ennemi et profitent de la charge émotionnelle d'une « menace fondamentale », le défi posé par la désinformation dépasse la menace qu'un seul acteur pernicieux peut représenter. Les historiens qui auront accès à diverses archives jugeront du degré de prescience des autorités britanniques dans leur réponse à l'activité russe. Mais la hausse de la désinformation numérique – qu'elle soit poussée par des acteurs étatiques ou non – est un problème de réseau et, pour cette raison, elle nécessite une réponse en réseau. De même que la sécurité physique au XXIe siècle, la sécurité réputationnelle induit un travail d'équipe. Les réponses coordonnées par des initiatives collectives telles que l'effort de l'Union européenne pour lutter contre la désinformation, le travail du Fonds européen pour la démocratie, et les partenariats sur le terrain avec d'autres acteurs internationaux cherchant à développer les institutions de la société civile seront probablement plus heureux que les discours cocardiers des chefs de gouvernement et du renseignement ou que les initiatives unilatérales des plateformes de réseaux sociaux. Ceci dit, les répercussions du piratage d'Integrity Initiative soulignent l'importance de partenariats transparents[64].

Ensuite, nous devons garder en tête que les canaux les plus propices aux incursions des guerres de l'information sont les failles créées par nos propres sociétés. Il n'y a pas de honte à tirer des enseignements des pistes offertes par les médias de l'adversaire et à chercher à corriger ces éléments d'insécurité réputationnelle. L'universitaire Mary Dudziak a bien montré que, si le président Eisenhower avait souhaité trouver une réponse rapide aux défis posés par le mouvement des droits civiques dans les années 1950, c'était tout autant à cause des pressions exercées par les membres du mouvement qu'à cause de celles de l'Union soviétique dans les médias internationaux[65]. Ainsi, une nation devrait faire tout ce qui est en son pouvoir pour éviter de confirmer les stéréotypes perpétués par les médias de ses adversaires. Le Royaume-Uni attaque fermement l'idée que « l'Ouest » serait tout autant corrompu que « l'Est » mais il serait plus crédible si Londres n'était pas le refuge préféré de tout oligarque qui souhaite déguster une boîte de Privé Beluga en paix. Finalement, le soutien apporté aux alliances stratégiques serait plus vraisemblable si le Royaume-Uni ne quittait pas l'Union européenne.

Le contenu des messages britanniques doit être préparé avec soin. La sécurité réputationnelle demande à la fois sagesse et honnêteté. Alors que les relations internationales connaissent une détérioration certaine, la tentation est forte de diaboliser non seulement un leadership politique, mais également un pays tout entier. Diaboliser ainsi tout le peuple russe – ou tout autre peuple présenté comme un adversaire – donne plus de prégnance à ceux qui soutiennent que l'on ne peut faire confiance aux étrangers car ceux-ci ne cherchent qu'à accaparer une admiration internationale due à un autre. De la même manière, il est important de ne pas faire la « promotion » de ses valeurs au-delà du raisonnable. Vasily Gatov a noté que la férocité de la bataille informationnelle actuelle vient en partie de la désillusion des journalistes russes qui ont répondu à l'appel de l'Ouest dans les années 1990 et accepté des emplois à CNN et NBC à Moscou… pour finalement

s’y brûler les ailes[66]. Le poète anglais William Congreve notait en 1697 que « le Paradis ne connaît de colère plus forte qu’un amour devenu haine[67] ».

Finalement, la tentation de mêler un orgueil géographique à un discours sur la protection des droits de l’homme est un élément problématique de la rhétorique occidentale. Des notions telles que les « valeurs euro-atlantiques » mettent à l’aise les responsables politiques lors des sommets de l’OTAN, mais elles cachent le travail de tous les pays qui œuvrent à mettre en pratique les droits garantis par la Déclaration universelle de 1948 – et l’influence de toutes les grandes traditions intellectuelles et culturelles dans ce document. Accaparer l’approche des relations internationales fondée sur les droits fait ainsi le jeu des acteurs politiques qui présentent ces droits comme des valeurs étrangères et non des droits inhérents à leurs populations.

*

Si l’époque actuelle est marquée par la transformation de l’information en arme, le chemin de la sécurité passe naturellement – comme avec toute arme – par un processus de désarmement. Le désarmement de l’information a fait preuve de son efficacité dans le passé. On le retrouve dans la phase de réconciliation à la fin de la guerre froide à travers des discussions sur l’utilisation des stéréotypes, la correction des manuels scolaires, et des rencontres entre citoyens des deux superpuissances. Des négociations sur les conséquences non communicationnelles ont par ailleurs été efficaces. La réponse la plus forte à l’idée véhiculée par le KGB qu’un laboratoire de l’armée américaine avait créé le sida a été de menacer Mikhaïl Gorbatchev de suspendre l’aide scientifique américaine fournie pour lutter contre le VIH si le gouvernement soviétique n’arrêtait pas de promouvoir cette idée[68]. À ce jour, la volonté de s’engager dans un cyberdésarmement est inexistante. La course à la suprématie numérique demeure la priorité.

Au-delà de tout processus bilatéral de désarmement, nous devons garder à l'esprit que le mécanisme sous-jacent qui valorise la désinformation est la capacité à détourner le statut de victime à son avantage. Les nouveaux hommes forts qui défient actuellement le système international ont promis à leurs citoyens qu'eux seuls étaient en mesure de réparer les injustices passées dont ils avaient souffert : « rendre sa grandeur » à un pays, rétablir le respect, ou « reprendre le contrôle ». Ces messages partout renforcent ce statut de victime que l'on se représente, en rappelant au citoyen d'un pays X de voter pour l'indépendance vis-à-vis d'un pays Y ou de quitter telle alliance Z. On se souvient que ces mêmes récits de victimisation justifiaient les nettoyages ethniques des années 1990 et l'extrémisme religieux des années 2000. Il est maintenant temps de trouver comment faire face à notre addiction collective au statut de victime et ainsi donner à ces récits la même attention que la radicalisation et la violence extrémiste ont reçue au début des années 2010. La manière la plus efficace de s'attaquer à un discours clivant fondé sur le passé est d'offrir un discours orienté vers l'avenir qui serait inclusif et nettement plus séduisant. Une telle approche a permis au monde de se dégager des trois grandes crises du XX^{e} siècle – deux guerres mondiales et une guerre froide – et il est grand temps d'offrir à l'humanité une vision de ce qu'elle pourrait devenir : notre futur en dépend [69].

Pour aller plus loin

CULL Nicholas J., *Public Diplomacy : Foundations for Global Engagement in the Digital Age*, Cambridge, Polity, 2019.

PAMMENT James, *British Public Diplomacy and Soft Power : Diplomatic Influence and the Digital Revolution*, Londres, Palgrave, 2016.

POMERANTSEV Peter, *This Is Not Propaganda : Adventures in the War Against Reality*, Londres, Faber & Faber, 2019.

SUROWIEC Paweł et MANOR Ilan (dir.), *Public Diplomacy and the Politics of Uncertainty*, New York, Palgrave, 2020 (à paraître).

SUROWIEC Paweł et LONG Philip, « Hybridity and soft power statecraft : The "GREAT" Campaign », *Diplomacy and Statecraft*, 2020, vol. 31, n° 1, p. 168-195.

CHAPITRE 10

Les États-Unis : la militarisation de la diplomatie publique

Maud Quessard

En février 2019, le *Washington Post* annonçait, ce que les milieux politiques américains espéraient depuis plusieurs mois, que l'armée américaine aurait réussi, à l'automne 2018, à « débrancher l'IRA » (l'Internet Research Agency[1]). Il s'agissait de protéger le bon déroulement des élections de mi-mandat (*Midterms*) aux États-Unis, en empêchant de nuire ceux-là mêmes que la justice américaine avait rendus responsables d'ingérence dans la campagne présidentielle de 2016[2]. Ce prétendu scoop journalistique, largement relayé par les médias internationaux et les réseaux sociaux, venait confirmer une rumeur entretenue depuis plusieurs semaines à Washington sur les capacités du Cyber Command (le commandement cyber américain) et de la NSA (National Security Agency) à pratiquer des opérations « musclées » de lutte offensive contre d'éventuels hackers liés au Kremlin[3]. Cette opération s'inscrivait dans un effort plus large de l'ensemble du gouvernement américain, appelé « interagence » (interministériel pour son équivalent français), pour contrer l'influence russe dans le processus électoral de 2018[4]. Cette opération d'intimidation a

pris la forme d'une campagne de *messaging* numérique à destination des hackers présumés dans le but de les « dissuader d'interférer dans le processus électoral en ayant recours à la désinformation[5] ».

La « campagne d'information » autour de cette manifestation de force dans l'espace cyber traduisait la volonté du gouvernement américain de communiquer sur la capacité d'intimidation ou de dissuasion (*deter*) des États-Unis dans le 5e domaine de lutte identifié par la doctrine américaine (Terre, Mer, Air, Espace, Information)[6]. Elle illustrait également l'évolution du débat public autour des opérations d'information (*Info Ops*) et des opérations de lutte informatique qui sont devenues des outils privilégiés de la guerre psychologique[7].

Si l'on s'intéresse à l'évolution des pratiques de la politique étrangère américaine à l'ère numérique, on comprend rapidement que, conformément au poids du Pentagone dans cette organisation, une large place soit faite à la militarisation de l'information[8]. Comme le montrent les travaux récents menés par le Congrès[9], il n'existe pas véritablement de doctrine homogène en matière de contre-propagande américaine. Pour le Pentagone, c'est la première guerre du Golfe en 1991 qui entraîne une révolution des affaires militaires sur le plan informationnel ; elle est perçue comme la première guerre de l'ère numérique. La doctrine la définit alors comme « l'ensemble des actions ayant pour but d'acquérir une supériorité informationnelle en influençant l'information de l'adversaire, ses processus et systèmes à base d'information, ainsi que ses réseaux informatiques, tout en défendant et protégeant les siens[10] ».

Dans le cadre des nouvelles compétitions de puissance définies dans les documents stratégiques américains de 2017 et 2018 (*National Security Strategy*, *National Defense Strategy*, *National Cyber Strategy*), les guerres du XXIe siècle se jouent sur de nouveaux terrains de conflictualité, en dessous du seuil de « la guerre totale », dans « la zone grise » (*gray zone*)[11]. Les guerres de l'information contemporaines aux États-Unis, *information*

warfare (IW), désignent deux types d'actions : des programmes d'information gouvernementaux et des opérations militaires. En d'autres termes, elles représentent l'ensemble des stratégies mises en œuvre (défensives ou offensives) pour acquérir un avantage comparatif au sein de « l'espace informationnel ».

Bien que l'information soit considérée par la doctrine comme un pilier de la puissance et un élément-clé pour la sécurité nationale, le concept de guerre de l'information était jusqu'en 2017, assez mal connu et mal employé au sein des milieux institutionnels[12]. La loi d'autorisation de la Défense nationale de 2017 précise la nature des menaces informationnelles auxquelles les États-Unis sont confrontés et contre lesquelles les organismes institutionnels doivent lutter en priorité. Les propagandes d'États comme la Russie, l'Iran, la Chine puis la Corée du Nord sont considérées comme les plus nuisibles ; les propagandes des groupes djihadistes incluant Daech demeurent classées juste derrière la Russie[13].

Ce chapitre aura pour but de montrer comment la diplomatie publique, pratique idoine du département d'État, héritée de la guerre froide s'est fortement militarisée à l'ère numérique. Il apportera un éclairage sur les points suivants : l'évolution de la terminologie et de la doctrine américaine à l'époque contemporaine, le rôle des acteurs institutionnels, opérationnels ou privés face aux nouvelles menaces informationnelles, la vulnérabilité des infrastructures numériques de l'État américain.

Le virage numérique de la diplomatie publique de Bush à Obama

Après les attentats du 11 septembre 2001, les autorités américaines doivent faire face à une crise de défiance vis-à-vis du leadership américain,

alors que la révolution numérique accélère le bouleversement des modes de communication et les équations de la diplomatie publique. Les responsables politiques américains prennent alors conscience qu'il est nécessaire de moderniser leurs outils et leurs pratiques du *soft power* gouvernemental, en prenant le virage numérique pour faire face aux défis posés par les mutations des guerres de l'information contemporaines. Les stratégies de l'adversaire, groupes djihadistes puis États concurrents des États-Unis (Russie, Chine, Iran, Corée du Nord), se concentrent sur des segments, des groupes ou des individus déjà identifiés comme favorables ou acquis, a priori, à leur message, en jouant sur le phénomène de balkanisation des opinions publiques, favorisé par les plateformes Internet et les réseaux sociaux[14]. La diplomatie publique paraît être alors un outil indispensable à la reconstruction et à la diffusion d'une image positive de l'Amérique à l'étranger.

Des médias traditionnels aux réseaux sociaux

Jusqu'aux attentats du 11 septembre 2001, le volet médiatique de la diplomatie publique s'était concentré sur les médias traditionnels, hérités de la guerre froide et regroupés au sein du Broadcasting Board of Governors (BBG)[15], agence responsable de la coordination des médias d'État américains comme Voice of America (VOA), Office of Cuba Broadcasting (OCB), Middle East Broadcasting Network (MBN), Radio Asia (RA), Radio Marti et les « radios libres » Radio Free Europe et Radio Liberty (RFE et RL), très influentes durant la guerre froide mais tombées en désuétude face aux plateformes Internet.

Le département d'État doit son passage à l'ère numérique à James Glassman, sous-secrétaire d'État à la diplomatie publique de l'administration Bush. En 2008, il multiplie les initiatives pour tenter de « révolutionner la conquête des esprits », en utilisant les nouvelles

technologies et les réseaux sociaux pour soutenir les initiatives de la société civile[16]. Il cherche notamment des relais d'opinion sur Internet. Parmi ces porte-parole, des acteurs privés, des groupes antiterroristes tels que SAVE (Sisters Against Violent Extremism, « Les sœurs contre l'extrémisme violent »), sont créés en octobre 2008.

À l'heure de la société civile de l'Internet 2.0, le meilleur moyen pour le gouvernement américain de promouvoir la démocratie, les droits de l'homme ou de lutter contre la censure est de donner le pouvoir de communiquer le plus largement possible à des acteurs-clés de la société civile, vecteurs de changement. Alors que les États-Unis s'enfoncent dans la guerre en Irak et en Afghanistan, cette transformation marque le passage de l'État-nation à l'État-réseau (*Network State*[17]), annoncé comme inéluctable par plusieurs politologues américains[18]. Cette mutation est théorisée au niveau gouvernemental sous le nom de « l'État du XXIe siècle » (*21st century statecraft*)[19], nouvelle marque de l'Amérique, dont Hillary Clinton devient la figure de proue de l'administration Obama.

Information et « liberté d'Internet »

Au cours de la première décennie du XXIe siècle, la digitalisation de la diplomatie publique est perçue comme une révolution nécessaire pour maintenir le leadership américain dans un monde en réseau. Dans ce but, le département d'État est réorganisé ; il fait une place de choix aux professionnels des réseaux sociaux, en l'occurrence Alec Ross et Jared Cohen, élus parmi les 100 personnalités les plus influentes au monde par le magazine *Time* en 2013.

La diplomatie publique digitale au sein du département d'État se compose d'une équipe de bloggeurs qui postent régulièrement des messages ou tweetent pour rendre compte de ses activités. En tout, ce sont plus de 150 personnes qui appartiennent à l'équipe des diplomates des nouveaux

médias à Washington, alors que sur le terrain, dans les ambassades et les consulats, les *public affairs officers* de l'ère numérique ont pour mission de suivre et de participer aux flux de messages des réseaux sociaux locaux ou transnationaux. Le département d'État affiche alors fièrement ses 2,6 millions de followers sur Twitter (pour 301 détenteurs de comptes) et 15,5 millions d'amis sur Facebook (pour les 408 comptes du département d'État).

Pour certains observateurs étrangers, Alec Ross, conseiller pour l'innovation d'Hillary Clinton, façonne le *soft power* numérique des États-Unis en une arme de guerre lors des révolutions arabes. Lorsqu'il tweete, en pleine révolution égyptienne, « les citoyens doivent avoir le droit de critiquer un gouvernement sans peur de représailles », ses followers, parmi les insurgés, ont pu croire à un soutien de la puissance américaine. L'objectif affiché de la diplomatie publique américaine 2.0 est alors de promouvoir la démocratie en encourageant la « liberté d'accès à Internet » devenu « l'espace public du XXIe siècle ». Son rôle serait d'assurer, dans des pays comme l'Iran, la Chine, mais aussi Cuba, la Birmanie, la Syrie ou encore le Vietnam, l'accès à l'ensemble des ressources Internet et aux réseaux sociaux. L'utilisation des ressources numériques reflète « la puissance des technologies de connexion en tant qu'accélérateurs du changement politique, social et économique[20] ». Le département d'État ouvre des comptes Twitter en persan et en arabe pour communiquer directement avec les populations du Moyen-Orient. Des comptes en chinois, russe et hindi sont créés dans la même perspective.

Mike McFaul, ambassadeur des États-Unis en Russie, avec plus de 70 000 abonnés sur Twitter, est présenté comme un diplomate d'avant-garde. Il reste en contact direct avec la population russe *via* Twitter, alors que Vladimir Poutine restreint la liberté d'expression et demande la fermeture de l'USAID (United States Agency for International Development) à Moscou, en septembre 2012. De manière plus ciblée, le

département d'État développe des programmes de soutien à de jeunes militants jugés suffisamment crédibles pour influencer favorablement l'opinion dans leurs pays respectifs, réalisé en partenariat avec les GAFAM (Google, Apple, Facebook, Amazon, Microsoft). Il s'agit de soutenir les jeunes gens identifiés qui cherchent à utiliser les nouvelles technologies pour dénoncer les violences, et influencer les transformations à l'œuvre ou souhaitées dans leurs pays. Ils travaillent souvent dans des zones à risques (au Soudan, en Iran, en Égypte mais aussi en Europe de l'Est, au Venezuela ou en Thaïlande), et sont confrontés à des enjeux que les outils traditionnels de la diplomatie ne peuvent pas résoudre.

Le contrôle de l'information au cœur des enjeux de la diplomatie numérique

Cibler les dissidents, la jeunesse et les leaders d'opinion pour favoriser des stratégies d'influence de moyen ou de long terme, et participer aux changements de régime est une constante de la diplomatie publique américaine. Ce qui a changé, à l'ère numérique, ce sont les interactions possibles avec les individus et les groupes cibles, les interactions entre les officiels américains et leurs cibles, mais également entre ces groupes ou individus cibles eux-mêmes.

L'absence de contrôle est sans doute l'une des caractéristiques majeures de la diplomatie publique 2.0. Les professionnels de la diplomatie digitale en sont particulièrement conscients, il n'y aurait pas d'avenir pour les révolutions digitales sans leader d'opinion capable d'incarner le passage de la simple contestation à l'action politique, et les outils numériques ne pourraient que contribuer à les identifier[21]. La seconde caractéristique du passage à la diplomatie publique numérique pour les États-Unis a été la création de partenariats visibles avec les acteurs de la société civile

mondialisée, qui partagent leur point de vue et sont susceptibles de servir leurs intérêts.

Enfin, les GAFAM sont devenus des partenaires incontournables pour soutenir et préserver « la liberté d'Internet », ambition revendiquée par le département d'État. Ces partenariats permettent aussi de renforcer le *soft power* américain à moindre coût, dans un contexte de réductions budgétaires toujours accrues pour le département d'État au profit du Pentagone.

L'information comme vecteur d'influence militaire

Pour le Pentagone, le cœur de la guerre de l'information réside dans la collecte, la transmission et la rétention d'informations de manière à améliorer le processus décisionnel ou à détériorer celui de l'ennemi. Au cours de son histoire, l'armée américaine pour parvenir à ces finalités a eu recours à différents « moyens de communication », comme les opérations de guerre psychologique, la manipulation des médias et les campagnes de désinformation, mais aussi la guerre électronique ou les opérations cyber. Réussir à coordonner l'ensemble de ces actions a représenté un enjeu de taille pour les responsables de l'armée dont le premier manuel doctrinal à adopter une approche holistique des opérations d'information n'est paru qu'en 1996. C'est seulement en 2008 que la doctrine militaire a pu clarifier à nouveau sa terminologie alors que les guerres de l'information s'intensifiaient dans l'espace cyber[22].

Après les attentats du 11 septembre 2001, en l'absence d'un arsenal de diplomatie publique adapté à la guerre idéologique menée par les groupes jihadistes al-Qaida puis Daech, les capacités américaines de contre-

propagande militaire se sont essentiellement organisées autour des opérations d'information (*Information Operations*, OI). Le manque de moyens du département d'État, la transformation des ambassades en forteresses (pour lutter contre les risques d'attentats), ou la disparition de postes diplomatiques et d'agents de terrain (*public affairs officers*[23]) sur les théâtres d'opérations les plus brûlants ont favorisé la militarisation de la diplomatie publique comme sa numérisation.

Bien que le Pentagone s'en défende, la réalité des actions menées sur le terrain et dans le cyberespace confirme que la diplomatie publique est devenue partie intégrante de la communication stratégique américaine. L'ensemble de ces actions pensées et élaborées à la fois au niveau national, à Washington, et au sein des commandements militaires sur les différents théâtres d'opérations[24] peut paraître redondant ou contre-productif, ce qui génère des débats interagences sur les répartitions des responsabilités de la réponse ou de l'attaque, l'efficacité, et le coût des activités de diplomatie publique et d'influence militaire[25].

Enjeux politiques et pratiques militaires

Les débats doctrinaux contemporains relatifs à l'emploi des outils numériques dans les guerres de l'information interrogent notamment le rapport entre les opérations d'information (IO) et les opérations cyber (*Cyberspace Operations*, CO). Depuis une dizaine d'années les responsables du Conseil national de sécurité (NSC) considèrent que les opérations cybernétiques offensives (ou de lutte, suivant la terminologie française) doivent être distinguées des opérations d'information, de guerre psychologique ou de guerre électronique. Autrement dit, la formule *information warfare* comprend aujourd'hui les opérations d'information et d'influence (guerre psychologique) qui seraient à distinguer des opérations

cybernétiques[26]. En pratique cette distinction est particulièrement mince et elle n'est pas partagée par les acteurs de terrain.

Pour les responsables politiques à Washington, il est apparu éthiquement nécessaire de distinguer le *hacking* ayant une visée politique et constituant une forme d'espionnage légitime, du *hacking informatique* illégitime ayant une visée offensive[27]. Cette distinction politique (qui pose des questions juridiques) apparaît artificielle au regard de la pratique des opérations militaires américaines consistant en une intrusion dans un système informatique. Le plus souvent c'est uniquement l'intention qui distingue l'espionnage par voie numérique (collecte d'informations, renseignements sur l'environnement précédant une intervention militaire dans l'espace physique) de l'opération visant à nuire ou à détruire (*cyber effect operation*)[28]. La nécessité de distinguer les deux a suscité de nombreux débats entre le pouvoir politique et le Pentagone ou les responsables du renseignement au plus haut niveau, comme la controverse qui a opposé le président Obama en 2015 au responsable du renseignement américain, James Clapper, au moment même où les opérations d'information hostiles, notamment chinoises et russes, se multipliaient à l'encontre du territoire national[29].

Sur le plan sémantique, la communication stratégique américaine désigne à la fois des opérations d'information (*Information Operations*, IO) et des programmes d'engagement plus larges proposés par les *Public Affairs Officers*. Le département de la Défense soutient les activités de diplomatie publique[30] en sécurisant l'utilisation des réseaux sociaux (Twitter, Facebook) pour les diplomates qui pratiquent la diplomatie en temps réel (*real time diplomacy*[31]) ou qui diffusent leur message promotionnel et s'exposent aux risques de cyberattaques.

Cette intrusion relative des opérations de défense dans les prérogatives de la diplomatie publique a suscité des critiques et la méfiance de membres du Congrès. Les détracteurs de ces pratiques mettent en cause la perte de

légitimité et de crédibilité de ces opérations d'influence auprès des publics visés[32]. Il existe en effet des précédents malheureux comme l'OSI (Office of Strategic Influence), mis en place par Donald Rumsfeld en 2001, puis démantelé pour ces mêmes raisons après qu'on a accusé ses agents de fournir de fausses informations aux médias traditionnels, et donc de pratiquer la désinformation.

Le rôle fondamental des acteurs de terrain

Si les acteurs institutionnels à Washington insistent sur le caractère politique des guerres de l'information et se préoccupent de la dénomination des opérations d'information, de leurs enjeux juridiques, et des stratégies de réponse, les acteurs de terrain se soucient plus particulièrement des questions tactiques et de l'efficacité des opérations menées. Dans les guerres de l'information discrètes (ou à « empreinte numérique légère » pour reprendre l'expression *small foot-print*) menées sur les théâtres d'opérations, la taille réduite des unités opérationnelles est un atout majeur. Par ailleurs moins contraintes par le droit américain dans le cadre des opex, ces unités peuvent agir avec plus de célérité.

Aussi existe-t-il un découplage entre les stratégies et les actions des agences fédérales et celles des acteurs de terrain qui sont élaborées au sein des centres interarmées appelés COCOMs. Les opérations cyber offensives ne visent pas seulement à défendre le territoire national mais à faciliter la réussite des opérations militaires et à recueillir du renseignement. Pour la réussite de ces opérations, la question de la finesse du ciblage est cruciale, elle nécessite en amont une maîtrise des méthodes employées par les équipes dédiées (lors de la phase de préparation des opérations) et une évaluation des visées et des effets de ces opérations devenues « cyber guerre psychologique ».

La maîtrise des effets et des impacts sur les groupes cibles est donc au cœur des préoccupations tactiques des acteurs de terrain qui distinguent les campagnes à large spectre des opérations à visée réduite (individu, ou groupe précis). Les campagnes à large spectre sont souvent pensées dans le but de s'assurer du soutien des populations locales, des groupes cibles, des individus considérés comme des relais d'influence. Il existe des précédents, ceux de la guerre en Irak, en 2003, pour laquelle les opérations de guerres psychologiques (*Mission Accomplished* et *Coalition of the Willing*) dans le cadre des opérations d'information ont été un échec, tant les équipes américaines ont été rapidement dépassées par le monopole d'al-Qaida. En Afghanistan les retours d'expérience de l'opération *Enduring Freedom* ont permis d'esquisser une évaluation des opérations d'influence *via* les outils numériques menées depuis un théâtre d'opérations. Il en ressort que les campagnes d'information et d'influence étaient totalement inadaptées à l'environnement culturel afghan, notamment parce que les populations ciblées, souvent illettrées, avaient avant tout une culture orale et non numérique.

Forts de ces expériences, les acteurs opérationnels admettent aujourd'hui que l'organisation d'une campagne d'information *via* les réseaux numériques nécessite une préparation documentée du ciblage des populations au même titre qu'une campagne d'information utilisant des médias traditionnels. Ce n'est pas la quantité ou la fréquence des flux d'information diffusés *via* les réseaux qui garantit leur impact, dans ce cas l'effet recherché a pu être considéré comme nul.

À l'ère numérique, les opérations de terrain visant à influencer les populations étrangères se heurtent à deux écueils : sur le plan technique, elles n'échappent pas à la problématique de la vitesse, celle des attaques et du temps de réponse que nécessite une opération de contre-propagande soumise à approbation hiérarchique (comme c'est le cas fréquemment lors d'attaques cyber contre la radio la Voix de l'Amérique – Voice of America,

VOA[33]). Compte tenu de l'ensemble de ces difficultés, les forces spéciales sont demeurées jusqu'à présent les acteurs idoines pour mener des opérations tactiques de lutte informationnelle susceptibles d'atteindre l'objectif fixé[34].

Le manque de coordination des acteurs

À Washington, à la suite des accusations d'interférence russe dans le processus électoral américain de 2016 et à l'implantation, aux États-Unis, de médias d'État russes (Sputnik et Russia Today), les responsables politiques américains se sont interrogés sur leurs capacités de riposte et ont envisagé de restaurer des dispositifs de guerre froide. Ces inquiétudes ont traduit une préoccupation plus profonde qui est partagée dans les milieux diplomatiques et militaires, celle d'un manque de préparation et de coordination pour engager une riposte adaptée et proportionnelle aux nouvelles menaces de type informationnel.

En 2016, le Congrès avait autorisé le remplacement du Centre de communication stratégique contre le terrorisme (Center for Strategic Counterterrorism Communications) par le Global Engagement Center (GEC) au sein du département d'État pour lutter contre la propagande de Daech. Il s'agissait d'adapter les stratégies de contre-propagande et de diplomatie publique au nouvel environnement informationnel, en assurant la coordination d'un grand nombre d'acteurs publics ou privés (agences para-gouvernementales, ONG, GAFAM). Ses partisans les plus fervents ont voulu en faire le principal organe de réponse aux activités subversives du Kremlin, mais ils se sont heurtés à la complexité de l'appareil bureaucratique américain.

Le GEC devait donc privilégier le travail entre les agences, entre le ministère de la Défense, la communauté du renseignement, la NSA, le Cyber Command, le BBG, le département d'État et les GAFAM[35]. Pourtant

dans les faits, le GEC est essentiellement constitué de personnels appartenant au ministère de la Défense (à plus de 60 %). Plus nombreux et mieux formés à ces problématiques que les agents du département d'État qui pâtissent depuis plusieurs années du manque de moyens accordés à la diplomatie publique par le Congrès, les agents du Pentagone, qu'ils soient militaires ou civils, ont pris les commandes de la fabrique de l'information américaine au niveau institutionnel.

Par ailleurs, la formation des diplomates n'inclut pas de préparation aux guerres de l'information et de sensibilisation suffisante au rôle des opinions publiques dans les relations internationales[36], contrairement aux nombreuses formations qui existent pour les militaires au sein du ministère de la Défense. Aussi déplore-t-on que la militarisation des enjeux de sécurité nationale conduise à un cloisonnement de l'information, et à une appréciation difficile des stratégies numériques par les diplomates dans les guerres dites « hybrides ».

Le manque de coordination entre les différentes institutions concernées est identifié comme la principale faiblesse du dispositif. Le GEC est constitué officiellement de soixante-dix personnes divisées en plusieurs unités régionales (parlant français, ourdou, arabe, etc.), dont une vingtaine d'analystes contractuels, une équipe dédiée aux questions numériques. Ses principaux succès résident, selon ses responsables, dans la lutte contre la propagande islamiste en faveur du djihad sur Internet. Les avancées sont moins significatives dans la lutte contre les stratégies cyber russes, iraniennes ou chinoises, face auxquelles de 2008 à 2017, le gouvernement américain a favorisé l'observation de ces phénomènes, et les stratégies défensives. Aujourd'hui le GEC est considéré comme un centre d'analyse de données (*data center*) peu à même de coordonner des programmes d'information et d'engagement utilisant les moyens humains et cyber.

Ces faiblesses ont aussi révélé le manque d'intérêt du président Trump pour les enjeux de diplomatie publique, et pour la nécessité de diffuser un

narratif national auprès des populations étrangères. Les outils numériques n'ont jamais tant été utilisés que sous l'administration Trump. Mais ils ont également consacré la faillite de la diplomatie digitale, celle des stratégies d'engagement *via* les outils numériques.

Les réponses institutionnelles aux guerres cyber

Pour pallier les échecs de la diplomatie numérique et sécuriser les infrastructures de leur appareil de défense et de renseignement, les responsables de la sécurité nationale des États-Unis ont dû opérer un changement de paradigme en passant d'une posture défensive à une posture offensive. L'acteur idoine de cette rupture (stratégique) manifeste entre l'administration Obama et l'administration Trump est sans conteste le Cyber Command.

Les vulnérabilités du géant militaire américain

La prise de conscience de l'amplification des menaces informationnelles et cyber (appartenant aux actions intermédiaires appelées aussi menaces hybrides[37]) conduites par des États adversaires des États-Unis a connu un tournant en 2008, lorsque Supernet, le système Intranet du Pentagone réputé inviolable, est victime de hackers à la solde du Kremlin. Des clés USB promotionnelles, laissées à dessein sur les parkings de bases américaines au Moyen-Orient, ont permis d'introduire un logiciel malveillant dans les ordinateurs de plusieurs employés et de voler des centaines d'informations et de communications secrètes.

À la suite de ces événements, les responsables de la sécurité nationale américains ont pris conscience que les questions de cyberespionnage ne

pouvaient plus être des préoccupations du seul renseignement américain, de la NSA, elles devaient être aussi une priorité des acteurs militaires. La réponse du gouvernement américain n'a pas pu être immédiate parce que cette intrusion inédite pour le Pentagone venait s'ajouter à la récente intrusion chinoise dans le système de Lockheed Martin qui avait permis aux hackers chinois de voler les plans des avions de chasse américains F-35.

Le Cyber Command était encore embryonnaire et sous la tutelle de la NSA. La crainte majeure des autorités américaines était alors que ces intrusions malveillantes permettent aussi de modifier ou de manipuler des informations ou des données sensibles, qu'il s'agisse de modifier le groupe sanguin de certains soldats dans la base de données du système de santé des armées ou la trajectoire d'un missile.

Dès l'élection du président Barack Obama, la question de la vulnérabilité des systèmes informatiques et de communication est posée. Tout l'enjeu consiste à avoir les capacités d'identifier ces menaces supposées ou avérées et à y apporter des réponses adéquates. En plus des menaces russes ou chinoises, les États iranien ou nord-coréen font aussi des démonstrations de force dans ce nouvel espace de conflictualité. Ils développent des cyberattaques de grande ampleur, dont un des exemples les plus médiatisés demeure le piratage de Sony Pictures Enternainment par Lazarus, un groupe de hackers pro-Pyongyang, à l'occasion de la sortie du film *L'Interview*, comédie au vitriol caricaturant la dictature nord-coréenne. La réponse gouvernementale prend la forme de sanctions commerciales et de coupures Internet ponctuelles. La réponse militaire américaine met quant à elle plusieurs années à s'organiser entre 2008 et 2014. Pendant cette période, il s'agit avant tout d'observer les méthodes de l'adversaire et de former des unités spéciales dédiées au cyber dont l'expertise doit venir renforcer progressivement les différents corps d'armée (Terre, Air, Marine).

Cette posture demeure, malgré l'amplification des attaques qui prennent la forme d'opérations ciblées contre les réseaux énergétiques américains

(nucléaires ou pétroliers). Jusqu'en 2016, la nature de la réponse ne semble pas proportionnelle à l'ampleur des menaces et actions concrètes employant les outils cyber pour des opérations informationnelles. La nomination du général Paul Nakasone à la tête de la NSA et du Cyber Command change cet état de choses.

L'affirmation d'une posture offensive

Interrogé en mars 2018 lors de son audition de confirmation au Sénat sur les représailles que les adversaires des États-Unis peuvent craindre selon lui après des attaques cyber ou informationnelles, le général Nakasone souligne que ceux-ci n'ont aucune crainte (l'effort de dissuasion serait insuffisant ou inefficace). Pour pallier cela, il applique officieusement un concept hérité des forces spéciales américaines, *Defend forward*, mis en œuvre dans la guerre contre le terrorisme, et qui consiste à mener des actions préventives en étant présents dans les systèmes informatiques étrangers en permanence[38]. En d'autres termes, il faut être prêt à l'offensive pour rendre la défense du territoire national efficace.

Aujourd'hui, le Cyber Command doté de nouvelles prérogatives par le président Trump (en vertu du *National Memorandum 13*[39]) et par le Congrès, mènerait des opérations cyber préventives ciblées sur des sites stratégiques étrangers (russes en priorité). Celles-ci ne seraient pas soumises à l'approbation préalable de la Maison Blanche, ce qui permet d'augmenter la rapidité des réponses. L'objectif de ces attaques préventives qui consistent à débrancher l'IRA ou à réaliser des campagnes de *messaging* ciblées à l'encontre d'officiels ou de militaires étrangers serait de dissuader l'ensemble des États menaçants pour la démocratie et la sécurité nationale américaine. Il s'agit d'étendre les pratiques de la « dissuasion » au domaine du cyber et de l'information.

Ainsi, l'intrusion américaine menée contre des infrastructures électriques russes en juin 2019 a été présentée publiquement comme un moyen de prévenir des coupures de courant massives dans certains États pivots américains, pendant la campagne présidentielle de 2020[40]. Pour les responsables des opérations cyber offensives américaines, le défi est désormais d'infiltrer numériquement les systèmes hostiles avant même que ceux-ci ne puissent attaquer le territoire national. L'objectif est aussi de faire croire à un équilibre des forces, d'accentuer la dissuasion comme au temps de l'ère nucléaire. Pour autant, l'idée est d'éviter pour l'ensemble des acteurs tout dommage atteignant des cibles civiles (comme les hôpitaux) pour éviter l'escalade.

*

Conscients des vulnérabilités de leurs infrastructures**,** les décideurs politiques et militaires se sont interrogés sur leurs capacités de riposte. Le département d'État étant affaibli par le manque de moyens accordés, *de facto* l'appareil de guerre psychologique de l'ère contemporaine est plus fortement militarisé, et les stratégies de riposte se heurtent à quatre écueils principaux : le déséquilibre des outils employés, le manque de coordination des stratégies retenues par les différents acteurs poursuivant un même objectif, la capacité à évaluer leur impact sur les publics ciblés, le contrôle de la communication numérique du président Trump[41].

Au terme du premier mandat du président Trump et de trois années de débats au Congrès, deux impératifs sont apparus. Tout d'abord, la nécessité de créer rapidement au niveau fédéral, un bureau de coordination de la communication stratégique, OSN (Office of Strategic Narrative) dépendant du Conseil de sécurité nationale (NSC), pour coordonner d'une part les *Psy Ops* et les *Public Affairs*, et d'autre part les interactions avec l'OTAN. Par ailleurs, les stratèges du Pentagone qui réfléchissent à l'amélioration de la doctrine et à l'accroissement de l'efficacité des actions offensives et

défensives appellent à l'instauration d'un Commandement de guerre informationnelle (*Information Warfare Command*), qui pourrait traiter de manière coordonnée l'ensemble des opérations d'information[42].

Ainsi le contexte politique américain contemporain est marqué par la défiance vis-à-vis de ce qui est présenté comme de nouvelles stratégies d'influence russes ou chinoises mais le problème est bien plus large, il concerne tous les acteurs de la scène internationale, étatiques ou non étatiques, disposant ou susceptibles de former une *CyberArmy* moins coûteuse qu'une armée conventionnelle. Les principales préoccupations américaines en matière de menaces numériques à l'horizon 2024 concernent, d'une part les acteurs étatiques (Chine, Russie, Iran, Corée du Nord), et certains alliés observés avec curiosité (Israël)[43], et d'autre part les acteurs non étatiques Daech et WikiLeaks.

Les États-Unis n'ont peut-être pas perdu les guerres de l'information mais ils ont perdu leur avantage comparatif sur la maîtrise des flux d'information et ont révélé la vulnérabilité de leurs systèmes numériques en cas de crise politique ou géopolitique. Les États-Unis de l'ère Trump seraient victimes des éléments-clés de leur propre *soft power.* Leur capacité à créer des technologies favorisant l'utilisation des outils numériques par leurs adversaires serait devenue le talon d'Achille de leur architecture de défense.

Pour aller plus loin

ARDIS John A. S., KEENE Shima D., *Maintaining Information Dominance in Complex Environments*, Carlisle Barracks, United States Army War College Press, 2018.

MAURER Tim, *Cyber Mercenaries : The State, Hackers, and Power*, Cambridge/New York, Cambridge University Press, 2018.

QUESSARD Maud, *Stratégies d'influence et guerres de l'information. Propagande et diplomatie publique des États-Unis depuis la guerre froide*, Rennes, PUR, 2019.

THEOHARY Catherine A., « Information warfare : Issues for Congress », Washington, National Security Policy, Cyber and Information Operations, CRS, 5 mars 2018.

SEIB Philip, *Real-Time Diplomacy : Politics and Power in the Social Media Era*, New York, Palgrave, 2012.

STENGEL Richard, *Information Wars. How We Lost the Global Battle Against Disinformation and What Can We Do About It*, New York, Grove Press, 2019.

PAUL Christopher, CLARKE Colin P., SCHWILLE Michael, HLÁVKA Jakub P., BROWN Michael A., DAVENPORT Steven S., PORCHE III Isaac R., HARDING Joel, *Lessons From Others for Future U.S. Army Operations In and Through the Information Environment*, Santa Monica, RAND Corporation, 2018.

CHAPITRE 11

Israël : de la *hasbara* à la guerre cognitive

Amélie Férey

Le 27 septembre 2012, à l'occasion du rendez-vous de l'Assemblée générale des Nations unies, le Premier ministre israélien Benjamin Netanyahou surprend l'audience en brandissant un panneau sur lequel est esquissée une bombe. Devant un parterre de chefs d'État médusés, il trace au feutre rouge une ligne ne devant pas être dépassée. Le croquis représente le programme nucléaire iranien contre lequel Israël alerte l'opinion internationale depuis 2002. Le caractère visuel et audacieux de cette démarche lui assure d'importantes retombées médiatiques. Devant un tel succès, Benjamin Netanyahou adopte cette technique de communication politique, exhibant un débris de drone iranien abattu par Israël[1], des clichés de « site de stockage atomique secret » à Téhéran[2], ou encore des classeurs et des disquettes aux données confidentielles[3]. Ces offensives médiatiques soulignent l'importance donnée à l'exploitation de l'information par l'État israélien, qui intègre dans sa doctrine militaire ce « quatrième front » ou « front des consciences »[4].

Cette prise de conscience de l'importance stratégique de l'information est d'autant plus forte qu'elle répond à un contexte international particulier.

L'État hébreu s'est efforcé de rompre son isolement au sein de l'Assemblée des Nations unies, par un travail de lobbying visant à sa « normalisation » dans le concert des nations[5]. Alors que vingt et un États membres de l'ONU ne reconnaissent pas son existence, Israël se conçoit comme une citadelle assiégée cernée par des pays hostiles remettant sans cesse en cause sa légitimité – une perception renforcée par les régulières déclarations en ce sens du Hezbollah libanais et de la République islamique iranienne. L'influence politique et militaire qu'offre la bonne gestion de l'information est donc, peut-être plus que pour d'autres pays, centrale pour la politique étrangère israélienne.

Afin de protéger ses intérêts sur la scène internationale, cet État s'est progressivement doté d'institutions militaires efficaces et politiques formées spécifiquement au maniement stratégique de l'information. Son efficacité à tirer parti des renseignements collectés s'explique par une stratégie informationnelle se divisant en deux volets. Le premier se concentre sur la communication politique, *via* la mise en œuvre d'une politique de *hasbara* qui cherche à expliquer la politique de l'État hébreu et qui plonge ses racines dans l'histoire du sionisme. Le deuxième se concentre sur l'emploi de l'information à des fins de guerre cognitive. Cependant, alors même qu'une partie conséquente de ses ressources est consacrée au contrôle des discours, Israël vit ses efforts dans ce domaine comme un échec constant[6]. Chaque intervention militaire est en effet abondamment commentée et critiquée au niveau international.

La *hasbara* et la communication politique

Le premier volet de l'effort israélien dans le domaine de l'information est caractérisé par une communication politique institutionnalisée, dont le but est d'« expliquer » sa situation au Moyen-Orient. Depuis sa création en

1948 jusqu'à aujourd'hui, Israël met un soin particulier à communiquer sur ses actions et à justifier ses éventuelles prises de décision auprès des États et acteurs de la scène internationale[7].

Les racines historiques du concept

La *hasbara*, qui signifie littéralement « explication » en hébreu, a pour objet de formuler de manière claire et percutante le point de vue de l'État d'Israël auprès de l'opinion publique internationale. Ce concept spécifique au mouvement sioniste et à l'État hébreu plonge ses racines dans l'histoire de la diaspora juive. Pour les Pères du sionisme, l'antisémitisme pouvait partiellement s'expliquer par une « mauvaise information » sur le peuple juif, que la *hasbara* avait pour mission de dissiper. Il était alors essentiel « d'expliquer » la position de la communauté juive afin d'assurer sa sécurité contre les préjugés antisémites[8]. Theodor Herzl détaille cette approche lors du premier Congrès sioniste de 1897 : « Depuis des temps immémoriaux, le monde a été mal informé à notre propos. […] Nous Sionistes désirons non une ligue internationale, mais une discussion internationale[9]. »

C'est toutefois le journaliste polonais Nahum Sokolow qui importe le terme dans le lexique sioniste, en estimant dès 1912 que « dans un avenir proche, l'opinion publique jouera un rôle décisif en ce qui concerne le gouvernement, la constitution, et tout le reste, et notre organisation [l'organisation sioniste mondiale], de son côté, ne peut rien faire de plus efficace que de se concentrer de manière permanente sur l'explication à grande échelle de ses aspirations fondamentales[10]. » Il échafaude une stratégie duale qui combine des efforts diplomatiques traditionnels dirigés vers les décideurs politiques à une diplomatie publique envers les leaders d'opinions, dont la *hasbara* actuelle s'inspire[11].

Entre propagande et diplomatie publique

Bien que le terme « explication » suggère une forme de neutralité, l'emploi de *hasbara* est aujourd'hui débattu. Selon que l'on se place ou non dans une perspective sioniste, on préférera parler de diplomatie publique ou de propagande. Le personnel politique israélien tend à employer la formule plus générique de diplomatie publique. L'ambassadeur Gideon Meir, directeur général du département des médias et des affaires publiques du ministère des Affaires étrangères israélien, précise que la *hasbara* « ne se réduit pas à de la propagande, ni à une tentative de simplement "expliquer" les politiques et la réalité israéliennes », concluant que le terme de « diplomatie publique serait probablement une formule bien meilleure[12] ». Cependant, la traditionnelle diplomatie publique ne parvient pas à embrasser le caractère protéiforme de la *hasbara*, qui cible simultanément les élites politiques, les faiseurs d'opinion et le grand public, et qui doit sa spécificité au fait d'être menée conjointement par des institutions gouvernementales, des organisations non gouvernementales, des groupes de pression et de simples citoyens, qu'ils soient étudiants, journalistes ou blogueurs.

Pour les critiques du sionisme, la *hasbara* désigne, au contraire, la propagande de l'État israélien. Le linguiste et philosophe Noam Chomsky met en garde contre son utilisation en expliquant que « le mot *hasbara* […] désigne la propagande israélienne, exprimant la thèse selon laquelle la position d'Israël est toujours juste, quelle que soit la question considérée, et qu'il est seulement nécessaire de l'expliquer[13] ». L'intellectuel palestinien Edward Said définit la *hasbara* par les actions et les faveurs qu'elle entraîne : « des déjeuners et voyages gratuits pour des journalistes influents ; des séminaires pour les étudiants juifs à l'université […] ; le fait de bombarder des membres du Congrès d'invitations à des visites ; des brochures et, surtout, de l'argent pour les campagnes électorales ; la direction (ou, selon le cas, le harcèlement) des photographes et des

intellectuels de l'Intifada actuelle pour produire certaines images et pas d'autres ; des conférences et visites touristiques organisées par d'éminents Israéliens ; la formation de commentateurs faisant fréquemment référence à l'Holocauste et à la situation d'Israël aujourd'hui ; de nombreuses publicités dans les journaux attaquant les Arabes et louant Israël ; et ainsi de suite[14] ».

Les thèmes développés depuis 1947 sont particulièrement récurrents, ce qui facilite leur diffusion. Il s'agit « d'expliquer » devant les audiences internationales qu'Israël est la seule démocratie du Moyen-Orient, que son armée respecte le droit international, qu'il n'y a pas d'apartheid et que la situation n'est pas comparable à celle de l'Afrique du Sud. Des brochures fournissant des arguments détaillés répondant à ces thèmes ont été distribuées en 2011 par le ministère de la Hasbara à destination des citoyens israéliens voyageant à l'étranger[15]. D'autre part, les réussites du pays sont mises en avant, notamment dans le domaine de la culture – le succès des séries TV israéliennes ou encore la tenue de l'Eurovision en 2019 à Tel Aviv, qui a été perçue comme une victoire de l'État hébreu dans sa volonté d'être « normalisé » sur le plan international[16]. De même, l'accent mis sur les prouesses technologiques d'Israël et la publicité de la *start-up nation* participent de cet effort de promotion d'une image positive du pays[17].

Des acteurs institutionnels nombreux

À cette permanence du message politique correspond une grande instabilité dans l'appareil institutionnel qui lui est dédié. Ce champ d'action a parfois été sous la compétence du ministère des Affaires étrangères par le biais de son service des médias et de la *hasbara*. Ce service a obtenu son indépendance avec un portefeuille dédié, sous la forme du ministère des Affaires stratégique en 2008 et de l'éphémère ministère de la Hasbara en

2011. En outre, le ministère du Tourisme, ainsi que celui de la Culture participent également à des activités *ad hoc* sur des projets spécifiques.

Ces institutions fonctionnent sous la houlette de la branche de *hasbara* rattachée au bureau du Premier ministre, tout en travaillant de concert avec le porte-parole de Tsahal, l'armée israélienne, et avec l'Agence juive. Enfin, une grande partie de ce travail de communication politique est effectuée par le biais d'organisations non gouvernementales telles que Stand With Us et The Israel Project en coopération avec l'État israélien, notamment par un système de financements publics[18]. Ces organisations produisent des ressources, comme des livrets, des diaporamas, des dépliants, des cartes et des sondages. Elles octroient aussi des bourses Hasbara à des étudiants internationaux et financent des projets aidant à diffuser une image positive d'Israël.

Le développement de la « guerre cognitive »

Cette attention prêtée à la communication politique se double d'efforts plus structurés pour formuler une stratégie de guerre cognitive, visant à atteindre des objectifs militaires par la formulation, l'exploitation et la manipulation des représentations d'acteurs préalablement identifiés.

De la guerre psychologique à la guerre cognitive

Dans le domaine militaire, le tout jeune État hébreu a d'abord eu recours à des méthodes somme toute classiques de guerre psychologique, dont le but est de dissuader les troupes adverses de prendre les armes. Par exemple, lors de la guerre d'indépendance de 1948, des tracts ont été largués tout au long de la route libanaise empruntée par les volontaires

irakiens et syriens se rendant sur les champs de bataille, posant la question suivante : « Pourquoi mourir sur un sol étranger[19] ? » L'objectif est alors de décourager l'ennemi de combattre, en questionnant l'objet même du conflit. Ces initiatives de guerre psychologique sont corrélées à la volonté plus large de manipulation (*deception*) visant à influencer la manière dont le personnel politique adverse perçoit Israël. Au sein de l'armée, l'unité Hatzav est chargée d'assurer une veille des médias arabes (presse, radio et télévision), qu'elle synthétise dans une enquête annuelle intitulée « Propaganda Lines » jusqu'au milieu des années 1970.

Aujourd'hui, les généraux préfèrent parler de « guerre cognitive », expression plus générale qui désigne les actions et outils non exclusivement militaires permettant d'influencer des audiences choisies. Un volume intitulé *The Cognitive Campaign : Strategic and Intelligence Perspectives*, publié conjointement par l'Institute for the Research and Methodology of Intelligence (IRMI) et l'Institute for National Securities Studies (INSS) en octobre 2019, prend acte de ce changement : la guerre cognitive est devenue au cours de la dernière décennie un élément central de la sécurité nationale israélienne[20]. Regroupant des contributions de personnalités de premier plan, le volume dresse le constat suivant : une stratégie cognitive efficace est composée d'un versant défensif visant à contrer l'emprise d'entités étrangères sur sa propre population et se double d'un aspect offensif dont l'objet est d'influencer les populations à l'international.

Le défi est alors de mener une campagne (contre-)cognitive interne et externe, sans heurter les institutions et valeurs démocratiques. Ne se cantonnant plus aux troupes ennemies, la guerre cognitive prend pour cible des populations civiles préalablement identifiées grâce à l'utilisation adéquate des nouvelles technologies. Elle ne se limite pas aux temps des conflits « ouverts », mais prend également place en période de calme relatif. Dans cette perspective, le but d'une campagne cognitive est de faire évoluer la perception d'une réalité chez un public identifié, afin de faciliter la

réalisation d'objectifs stratégiques ou opérationnels considérés comme cruciaux. Ces campagnes incluent des moyens de guerre psychologique connus et traditionnels, comme la dissuasion, le largage de tracts, l'utilisation de porte-parole, la mobilisation d'une diplomatie et la construction d'une influence *via* des médias de masse, comme la télévision et la presse. Elles s'appuient également sur des outils nouveaux provenant du monde digital, tels que les réseaux sociaux.

Le versant offensif : collecte de l'information et guerre cyber

Cette stratégie de guerre cognitive s'appuie sur la capacité de l'armée à collecter des informations – compétence qui échoit principalement à la Direction du renseignement militaire. Cette direction, l'une des plus anciennes de Tsahal, a été fondée dès la création de l'État. Elle comprend trois unités, dont la principale et la plus large est l'unité 8200[21]. Auréolée d'un mystère qui participe à sa sulfureuse réputation, l'unité 8200 est souvent citée comme étant à la pointe des techniques de guerre de l'information[22]. Elle est chargée de collecter l'information d'origine électronique, notamment en interceptant des communications privées et gouvernementales, afin de permettre de déjouer des attentats, de mener une guerre cyber et de recruter des informateurs. C'est elle qui serait à l'origine de l'opération *Olympic Games*, menée en collaboration avec les États-Unis et ayant pour objectif de retarder le programme nucléaire militaire iranien en implantant le virus informatique Stuxnet dans les centrifugeuses iraniennes du site de Natanz[23].

Ces impressionnantes capacités techniques soulèvent des interrogations sur la moralité des opérations qui y sont menées. Ainsi, en 2014, quarante-trois officiers et soldats réservistes de l'unité 8200 signent une tribune dans le quotidien *Yediot Aharonot* dans laquelle ils refusent publiquement de

« participer aux actions contre les Palestiniens et de continuer à être les outils du renforcement du contrôle militaire sur les territoires occupés ». Un des membres de l'unité raconte les méthodes contestables qui y sont pratiquées : « Si vous êtes homosexuel et que vous connaissez quelqu'un qui connaît une personne recherchée, Israël fera de votre vie un enfer. Si vous avez besoin d'un traitement médical urgent en Israël, en Cisjordanie ou à l'étranger, nous sommes à vos trousses. L'État d'Israël vous laissera mourir plutôt que de vous permettre d'obtenir un traitement médical si vous ne donnez pas d'abord des informations sur votre cousin, l'homme recherché. […] Dans le cours d'entraînement, nous avons appris et mémorisé les différents mots arabes pour dire homosexuel[24]. »

Le versant défensif : l'amélioration de l'image de l'armée

Sur le plan plus classique de la communication, l'armée israélienne prend soin de fournir aux médias étrangers des informations sur ses activités. Artisan de cette politique d'ouverture, Moshe Ya'alon est l'ancien chef d'état-major et ministre des Affaires stratégiques, puis de la Défense. Il s'est chargé de réformer l'armée israélienne en 2013 afin d'améliorer son image. Tout d'abord, il a cherché à maîtriser la communication opérationnelle. La réduction de la durée des commissions d'enquête en cas de litiges permet de garder la main sur la mise en récit d'une opération puisqu'elle accélère la publication d'une contre-version israélienne. De même, l'accueil de journalistes « embarqués » (*embedded*) pendant des opérations, la création d'un centre de données fiables et accessibles pour les médias étrangers ou encore le recrutement de volontaires pour « combattre » sur les réseaux sociaux permettent de conserver l'avantage dans la bataille de la communication. La culture militaire israélienne joue ici un rôle non négligeable : l'audace érigée en valeur de corps, mais aussi

la jeunesse des conscrits, rompus à l'emploi des nouvelles technologies, permettent d'innover en matière d'utilisation des réseaux sociaux.

Ensuite, la réforme a visé à améliorer le partage d'information entre l'armée israélienne, le ministère de la Défense, le ministère des Affaires étrangères et le ministère des Affaires stratégiques, ce qui a permis de fluidifier et de coordonner les informations diffusées sur les opérations militaires en cours[25]. Enfin, au centre de cette stratégie de communication se trouve l'unité de porte-parole, qui opère 24 heures sur 24. Elle est dotée d'un PC opérationnel (*war room*) qui centralise les progrès des opérations venant du front et en fournit une version officielle dans les meilleurs délais, et ce dans différentes langues. Sa réactivité et les importants moyens qui lui sont échus témoignent du choix fait par l'armée israélienne de communiquer largement sur les opérations qu'elle mène lorsqu'elle le juge opportun. Par exemple, l'assassinat ciblé d'Ahmed Jabari, le chef des brigades El Qassam du Hamas palestinien, ayant marqué le début de l'opération militaire à Gaza « Pilier de défense » en novembre 2012 a pu être suivi en temps réel *via* un *live tweet* de l'armée israélienne, un choix audacieux qualifié de « tournant dans la communication militaire[26] ».

Une telle ouverture a pour objectif de contrôler le récit qui est fait des opérations vis-à-vis de la presse internationale et du grand public, en s'assurant de sa primeur. Toutefois, ce pari de la transparence peut être à double tranchant. En 2009, l'armée israélienne publiait une vidéo d'une frappe de drone contre un camion transportant ce qui semblait être des roquettes Grad à l'est du camp de réfugiés de Jabalya dans le nord de Gaza. Or une contre-enquête menée par Human Rights Watch à partir des séquences vidéo révélées au public a apporté la preuve que les cylindres chargés à l'arrière du camion étaient en réalité des bonbonnes à oxygène, forçant l'armée israélienne à reconnaître son erreur[27]. Ce cas illustre les ambiguïtés de la bataille de communication que se livrent l'armée

israélienne et les organisations de défense des droits de l'homme présentes sur le terrain, qui dénoncent régulièrement des crimes de guerre.

Une combinaison d'approches contre l'Iran

La stratégie israélienne visant à contrer l'influence de l'Iran dans la région offre un exemple intéressant de conjugaison d'une politique de *hasbara* et d'une stratégie de guerre cognitive. Ce cas d'étude est révélateur de l'efficacité de la coopération entre les échelons politique et militaire en la matière. L'Iran occupe une place centrale dans l'agenda sécuritaire israélien depuis 2002, lorsque ce pays a révélé son intention d'obtenir la bombe nucléaire. Son idéologie révolutionnaire, conjuguée à sa volonté de détruire Israël, renforce la perception de menace de l'État hébreu. En outre, la doctrine Begin veut qu'Israël n'hésite pas à empêcher les pays voisins d'obtenir la bombe nucléaire, même si cela implique l'utilisation de la force militaire.

La stratégie informationnelle israélienne appliquée à l'Iran répond à quatre objectifs : mobiliser l'opinion internationale sur le danger d'un Iran nucléaire ; souligner les autres menaces que représente l'Iran, notamment par son soutien accordé à des organisations armées dans la région et par son programme de missile balistique ; menacer d'une attaque israélienne militaire sur les sites nucléaires iraniens ; délégitimer l'accord de Vienne sur le nucléaire iranien conclu en 2015[28]. Elle identifie différentes audiences-cibles : l'administration américaine, qu'il faut convaincre d'agir ; l'opinion publique américaine dont il faut s'assurer le soutien ; le régime iranien, qui doit être dissuadé par la menace constante de conduire des frappes aériennes ; les gouvernements étrangers, qu'il faut convaincre d'accroître la pression sur l'Iran et de l'isoler sur le plan international.

Les moyens mis en œuvre comportent des éléments de diplomatie publique, notamment l'utilisation de la page Facebook de Netanyahou, le

relais médiatique des rapports de l'Agence internationale de l'Énergie atomique, les discours dans des arènes internationales tels que les discours à l'ONU. Des éléments de langage rappelant la « menace existentielle » de l'Iran renforcent le sentiment d'urgence qu'Israël vise à instaurer. Ces efforts sont complétés par une stratégie offensive, notamment de guerre cyber. Elle prend la forme d'attaques menées par des pirates inconnus *via* des virus informatiques. En 2010, le virus Stuxnet, déjà mentionné, a réussi à provoquer des explosions dans les centrifugeuses de l'usine d'enrichissement d'uranium de Natanz. En 2011, des informations sensibles ont été volées par un virus espion baptisé Duqu. En 2012, le virus Flame a effacé les données d'installations pétrolières iraniennes, obligeant l'Iran à couper temporairement l'accès Internet de son industrie. Bien qu'Israël ne revendique pas officiellement ces attaques, les experts soupçonnent la participation de l'État hébreu à ces opérations qui nécessitent des ressources humaines et technologiques avancées[29].

Critique d'Israël ou faillite de la *hasbara* ?

La force de la stratégie israélienne d'exploitation de l'information tient à un réseau d'institutions politiques et militaires spécialement dédiées à cette question et capables de travailler de concert avec des acteurs privés dans le cadre de formules *ad hoc* lorsque cela est jugé nécessaire. Quel bilan peut-on dresser d'une décennie de guerre informationnelle ?

Certains des objectifs considérés comme primordiaux par l'État hébreu, notamment la lutte contre la nucléarisation de l'Iran et contre le mouvement Boycott Sanctions Désinvestissement (BDS), ont été atteints aux yeux du gouvernement israélien. Le ministre des Affaires stratégiques, dans son discours au Congrès allemand d'Israël (Deutscher Israelkongress) en novembre 2018, s'est ainsi félicité d'avoir mis le BDS sur la défensive[30].

En outre, la « normalisation » d'Israël, soit l'acceptation de sa légitimité sur la scène internationale, progresse. Les récentes prises de position des Émirats arabes unis et de l'Arabie saoudite pour une attitude plus bienveillante à l'égard d'Israël vont dans ce sens.

L'image dont ce pays jouit sur la scène internationale s'est améliorée au point d'en faire une destination touristique prisée. Ainsi, en 2019, le nombre de touristes a augmenté de 18 %, atteignant les 4,6 millions de visiteurs pour un pays de 8 millions d'habitants[31]. Enfin, la reconnaissance par les États-Unis de la souveraineté d'Israël sur le plateau du Golan et de Jérusalem comme capitale a couronné en 2018 les efforts menés de longue date par la diplomatie israélienne.

Comment dès lors expliquer la situation paradoxale de cet État qui, en dépit de ce bilan, se vit en situation d'échec permanent en termes de communication ? Les commentateurs israéliens sont, en effet, unanimes à ce sujet : Israël serait traité injustement sur la scène internationale car il serait tenu de respecter des critères moraux impossibles et que son armée serait scrutée et critiquée au moindre faux pas. L'annonce de la décision de la Cour pénale internationale d'ouvrir une enquête préliminaire engageant la responsabilité pénale d'Israël dans la colonisation est ainsi perçue comme un échec de la *hasbara*. En janvier 2020, le Premier ministre Benjamin Netanyahou a qualifié cette décision « d'attaque frontale » contre « le droit à se défendre des démocraties et le droit du peuple juif à vivre sur sa terre ancestrale, la terre d'Israël[32] ».

Cette perception reflète la tension qui existe entre les efforts considérables déployés par l'État hébreu au nom de la *hasbara* et le sentiment d'échec répandu dans le public israélien. Remarquons que ce constat pessimiste constitue en soi l'un des thèmes de la *hasbara*, qui est précisément justifié par la nécessité de défendre Israël contre des attaques perçues comme injustes. Le journaliste à *Haaretz* Anshel Pfeffer le déplore : « Les pratiquants de la *hasbara* – que l'on appelle *masbiranim* –

sont totalement convaincus de la véracité de leurs arguments. En effet, la *hasbara* est désormais l'un des principes fondamentaux du sionisme du XXIe siècle, un véritable acte de foi. » Il enjoint ainsi à ses concitoyens de ne pas prendre toute critique formulée à l'encontre d'Israël pour une faillite de la *hasbara*[33].

Pour aller plus loin

CUMMINGS Jonathan, *Israel's Public Diplomacy : The Problems of Hasbara, 1966-1975*, Lanham, Rowman & Littlefield, 2016.

KUPERWASSER Yossi, SIMAN-TOV David (dir.), « The cognitive campaign : Strategic and intelligence perspectives », INSS, Memorandum no 197, 2019.

SCHLEIFER Ron, *Psychological Warfare in the Arab Israeli Conflict*, New York, Palgrave Macmillan, 2014.

SHEIZAF Noam, « Hasbara : Why does the world fail to understand us ? », *+972 Magazine*, 2011.

Sites Internet :

https://www.gov.il/en/departments/Units//ministry_of_strategic_affairs_and_public_diplomacy

https://www.standwithus.com

CHAPITRE 12

Le Japon : une prise de conscience récente des enjeux informationnels

Valérie Niquet

Le concept de guerre de l'information (情報戦 *jôhôsen*) n'est utilisé au Japon que pour désigner les stratégies mises en place par d'autres puissances, au premier rang desquelles la République populaire de Chine (RPC) et la Russie. La dimension offensive de la guerre de l'information est a priori peu applicable au cas japonais. Une insularité encore très forte, en dépit de la globalisation, favorise le repli et une communication à vocation interne. L'objectif de toute action a longtemps été de satisfaire en priorité les attentes d'une hiérarchie bureaucratique peu investie dans les affaires extérieures qui ne touchent pas immédiatement aux intérêts du pays. Par ailleurs, comme pour toutes les grandes démocraties, la dimension offensive de la guerre de l'information, sous la forme de manipulation et d'ingérence directe dans les affaires intérieures d'autres puissances, ne constitue pas une priorité comme dans les régimes autoritaires qui défendent leur légitimité idéologique et leur survie existentielle dans un monde ouvert. S'ajoute à ces éléments dans le cas du Japon après la Seconde Guerre mondiale la volonté de rompre avec la propagande agressive de l'époque militariste.

En revanche, le Japon a développé une stratégie de communication et d'influence fondée sur deux éléments qui sont l'exploitation d'un *soft power* préexistant, et depuis l'arrivée au pouvoir du Premier ministre Shinzo Abe en 2012, le renforcement des objectifs et des moyens de la diplomatie publique[1]. Dans ce contexte, la distinction entre diplomatie culturelle et diplomatie publique est peu marquée. Dans l'objectif de mettre en avant son caractère « pacifique », la diplomatie publique après la Seconde Guerre mondiale s'est longtemps focalisée sur les éléments les moins controversés de la culture traditionnelle tels que l'art du thé ou l'arrangement floral (Ikebana).

En revanche la dimension défensive de la guerre de l'information au Japon est bien présente, appliquée au domaine d'Internet et de la guerre cybernétique, en s'appuyant à la fois sur l'élaboration de normes et le renforcement des capacités militaires défensives. Les entreprises privées, directement confrontées à ces défis, sont à la pointe de l'élaboration de nouvelles normes et de contre-mesures.

La puissance du *soft power* au Japon

L'importance du *soft power* japonais est indéniable dans la construction d'une image positive de la puissance japonaise, notamment en Occident. La caractéristique de ce *soft power* à forte dimension culturelle, est d'être issu de la société civile, et de susciter à l'étranger depuis plus d'un siècle (en dehors de la période de la Seconde Guerre mondiale) notamment auprès des élites occidentales, une force d'attraction longtemps relativement négligée par les autorités dans l'élaboration d'un discours de puissance. Au contraire, cette spécificité était destinée à renforcer l'image « pacifique » et non investie du Japon sur la scène internationale. Cette attractivité préexistante trouve désormais sa traduction dans la volonté du

gouvernement japonais de l'exploiter d'une manière systématique comme un instrument de sa stratégie extérieure[2].

Le Livre blanc sur la diplomatie publié en 2019 précise ainsi que le Japon doit « mettre en avant son attractivité fondée sur une culture riche et variée[3] ». Dès le début des années 2000, le Premier ministre Junichiro Koizumi avait lancé le concept de *cool Japan*, surfant sur cette popularité ancienne qui trouve un nouveau public grâce à la massification du marché de la culture *manga* à l'étranger, avec une dimension véritablement universelle, touchant les pays d'Asie autant que le monde occidental en dépit des tensions historiques, les élites comme la jeunesse.

À un autre niveau, le *soft power* du Japon permet l'exploitation de niches de politique étrangère telles que le pacifisme, le contrôle des armements ou les questions environnementales et climatiques, qui correspondent aux spécificités du Japon : le statut de victime des deux seuls bombardements atomiques de l'histoire et un attachement, présenté comme inhérent à la culture japonaise, à la « nature ». Cette stratégie de niche se traduit par des actions concrètes, telles que les discours des Premiers ministres à l'ONU, mais expose aussi Tokyo aux critiques portant sur ses choix en matière de dissuasion, qui repose sur le parapluie nucléaire américain, ou l'exportation de technologies de charbon propre, qui perpétue le recours aux énergies fossiles[4].

Pour Tokyo, la diplomatie culturelle et la diplomatie publique constituent deux éléments complémentaires et peu distincts au service de la promotion de la politique étrangère du Japon distincte des relations de gouvernement à gouvernement[5].

Une diplomatie publique plus active

Depuis le retour au pouvoir du Premier ministre Abe, le Japon a renforcé son discours de diplomatie publique, même si l'utilisation courante d'une transcription de l'anglais (パブリックディプロマシー *paburikku dipuromashi*) plutôt que le terme japonais (公共外交 *kôkyô gaikô*) montre les limites de l'intégration du concept à la culture diplomatique japonaise. L'objectif est « d'obtenir la compréhension et le soutien de la population au Japon et à l'étranger sur les questions de politique étrangère[6] ». Cette volonté a coïncidé avec celle d'accroître les moyens et la capacité d'action du cabinet du Premier ministre face aux bureaucraties traditionnelles, dont celle du ministère des Affaires étrangères à qui cette mission est également confiée. La mission du « bureau de communication » du Premier ministre, créé en 2011, est, entre autres, d'aider le monde extérieur à « comprendre le Japon ». L'accent est mis sur l'exploitation des « nouveaux » moyens de communication que sont les réseaux sociaux et Internet, ainsi que sur une présence accrue dans les médias étrangers[7].

Le discours de diplomatie publique du Japon insiste sur le partage de valeurs communes telles que la démocratie, le respect du droit, le non-recours à la force et la défense de l'ordre libéral international tel qu'il a été fondé après la Seconde Guerre mondiale. L'objectif est d'ancrer le Japon dans le « camp occidental » et démocratique, dans un contexte stratégique tendu face à l'émergence d'une puissance chinoise disruptive.

Ces objectifs ont été traduits avec succès dans des concepts opérationnels tels que celui de *Free and Open Indo-Pacific*, présenté par Shinzo Abe dès 2007 et formalisé en 2016, ou dans l'adoption la même année de lois de défense permettant de mieux intégrer les forces d'autodéfense aux opérations menées par les alliés dans ou hors du cadre des opérations de maintien de la paix de l'ONU.

Les questions territoriales, notamment celle de l'archipel des Senkaku, sujet de contentieux avec la RPC qui en revendique la souveraineté depuis les années 1970, constituent également un objectif de diplomatie publique

et font l’objet de communications accrues pour présenter la légitimité des positions du Japon[8].

Des moyens renforcés

Le Japon s’est doté de moyens conséquents destinés à renforcer sa puissance d’influence. Au sein du secrétariat du ministère des Affaires étrangères, il existe un département pour la presse et la diplomatie publique, qui comprend notamment une division pour la stratégie de diplomatie publique et une division pour les relations par Internet, ainsi qu’un département pour les affaires culturelles. Une liste concrète de missions qui consistent à « communiquer activement », « accroître les relations de peuple à peuple », y compris en « développant le tourisme », et développer les contacts avec les « leaders d’opinion, tels que les journalistes et les experts », a été définie.

La « marque Japon » (*Japan branding*) est mise en avant et Tokyo finance l’intervention de nombreux experts japonais venant encore très souvent du monde des « arts traditionnels », s’éloignant peu de l’image conventionnelle du Japon à l’étranger[9]. Le soutien à la participation d’experts venant du monde académique à des séminaires consacrés à des questions stratégiques d’actualité est toutefois en forte progression depuis les années 2010.

Destiné à soutenir cet effort, à la frontière entre l’économique et le diplomatique, le METI (Ministry of Economy Trade and Insdustry) a également créé le Cool Japan Fund en 2013 pour financer des projets avec des moyens publics et privés[10]. L’accent est mis sur les points forts traditionnels du Japon que sont les médias et leur contenu, en liaison avec l’industrie des mangas, la nourriture, la mode et le design. Certains critiquent des choix trop exclusivement focalisés sur l’image attendue du

Japon à l'étranger et un gaspillage d'argent public pour des projets qui ne sortent pas des secteurs traditionnels, sans contribuer à une meilleure compréhension des enjeux auxquels le Japon contemporain est confronté [11].

En 2015, le Japon a également décidé la création de trois « Maisons du Japon », à Londres, New York et São Paulo ; là aussi, l'accent est mis sur la culture et le style de vie, et les choix ne s'aventurent pas en dehors des zones de confort de l'action extérieure de l'archipel [12].

Les limites

Cette stratégie plus offensive en matière de diplomatie publique se heurte à plusieurs limites. La question de la langue est essentielle, avec à la fois un faible nombre d'acteurs maîtrisant parfaitement l'anglais du côté japonais, et un focus encore trop exclusif sur les États-Unis et la Grande-Bretagne, comme destinataires du discours. Si les États-Unis demeurent le principal allié du Japon, le choix de la Grande-Bretagne, dont l'importance et les moyens d'action ne peuvent se renforcer à l'heure du Brexit, est moins compréhensible. En la matière le poids historique des alliances communes autour des États-Unis l'emporte sur l'efficacité. Ce tropisme « anglo-saxon » et une moins bonne connaissance des autres acteurs au niveau stratégique expliquent également les choix de financement de chaires par le gouvernement japonais aux États-Unis et au Royaume-Uni alors qu'en Europe, l'UE joue un rôle croissant comme le montre la signature en 2019 d'un accord de partenariat stratégique entre Tokyo et Bruxelles.

Le deuxième écueil qui prolonge le premier est le poids de la bureaucratie des grands ministères – commanditaires et destinataires finaux – dans l'évaluation des actions menées. Souvent coupés de la réalité des perceptions et des modes de fonctionnement à l'extérieur de l'archipel,

ces organes peuvent nuire à l'efficacité des actions de diplomatie publique menées par le Japon. Les rivalités et l'absence de communication entre les différentes bureaucraties renforcent ces effets pervers. Le rôle leader du ministère des Affaires étrangères en matière de diplomatie publique et de diplomatie culturelle est souvent rappelé, mais les rivalités entre directions, notamment sur les questions budgétaires, pèsent sur l'élaboration d'une stratégie coordonnée.

L'absence de vision stratégique globale est notamment reflétée dans la faible présence de l'enseignement du Japonais, en dépit d'une attente très forte au niveau mondial. Le Japon ne dispose pas de l'équivalent de l'Alliance française, de l'Institut Goethe, du British Council et encore moins des Instituts Confucius[13]. Un autre effet pervers – quelle que soit la validité des positions de Tokyo en la matière – est le choix concomitant de thématiques contradictoires comme la question des femmes de réconfort ou des « réparations » avec la Corée du Sud, qui rappellent inopportunément la période militariste, et l'accent mis sur les valeurs universelles et le pacifisme, qui sont celles du Japon d'après-guerre.

Enfin, un attachement trop exclusif à la dimension culturelle, particulièrement dans des pays où ces relations culturelles sont anciennes comme la France, limite la compréhension et l'acceptation du Japon en tant qu'acteur stratégique significatif au niveau global.

Guerre de l'information et normes sur Internet

À la croisée de la « guerre de l'information » et du *soft power*, le Japon a toutefois fait de l'application des normes en matière cybernétique une nouvelle niche de diplomatie publique. Il s'agit de répondre à la « route de la soie digitale » que la RPC tente de mettre en place avec ses projets de

« connectivité ». Face à cette offensive technologique et idéologique de la Chine, le Japon déploie des moyens défensifs.

Le Premier ministre Abe a proposé lors du sommet du G20 d'Osaka en 2019 l'initiative « Osaka Track » sur « la libre circulation des données fondée sur la confiance », dont l'objectif est d'imposer des règles de transparence en matière de partage de l'information sur les données personnelles, la propriété intellectuelle et la sécurité cybernétique, y compris dans la mise en œuvre des réseaux 5G qui constituent un enjeu majeur avec la Chine.

Mais au-delà des normes et du *soft power*, le Japon s'est également doté de moyens défensifs militaires destinés à répondre aux techniques modernes de la guerre de l'information. En 2014, une unité de force interarmées de « défense cybernétique » a été créée au sein des forces d'autodéfense. En 2018, un état-major pour la défense cybernétique a été mis en place et cette unité a été portée à 1 000 hommes. Les *Defense Guidelines* 2018 prônent également de combiner les capacités des secteurs civil – particulièrement conscients des menaces – et militaire, pour renforcer les moyens de cette unité. Mais en la matière aussi, l'insularité du Japon pèse parfois sur l'appréciation des menaces. Les lacunes en matière de développement des usages d'Internet dans l'archipel, le vieillissement de la population et « l'obstacle » de la langue sont encore considérés comme des défenses suffisantes face aux stratégies de désinformation et de pénétration de réseaux en direction de l'archipel [14].

Le Japon est ainsi confronté à des défis majeurs, y compris en matière de guerre de l'information. Il fait également face à des obstacles qui rendent difficilement envisageable son passage d'un statut de *soft power* traditionnel à celui de *sharp power* offensif en matière de guerre de l'information [15]. Pour Tokyo, la dimension strictement défensive de la guerre de l'information est toujours mise en avant, même si les actions plus dynamiques menées en matière de diplomatie publique culturelle depuis le

début des années 2010 dénotent une volonté accrue de peser sur les prises de décision concernant ses intérêts dans un monde globalisé.

Pour aller plus loin

FISHLOCK Nicholas, « Policies to please political partners : The development of Japan's intelligence policy in the 21st century », Institute for Security and Development Policy (ISDP). Et pp.11, *Focus Asia*, juin 2019.

KINGSTON Jeff (éd.), *Press Freedom in Contemporary Japan*, Londres, Routledge, 2017.

PIKE John, *Japan Intelligence and Security Agencies*, Fas.org.

SNOW Nancy, *Japan Information War*, Create Space Independent Publishing Platform, 2016.

CHAPITRE 13

La France : quelle stratégie de résilience face aux manipulations de l'information ?

Benjamin Pajot

Si la société française n'a pas attendu le XXIe siècle pour découvrir la capacité de nuisance des ingérences étrangères dans le champ informationnel, il est néanmoins certain qu'en créant de nouvelles opportunités, la révolution numérique a depuis rebattu les cartes et induit de nouvelles menaces. L'avènement des réseaux sociaux a ainsi été associé au développement de nouvelles formes de guerre informationnelle « à l'heure d'Internet », auxquelles la France n'a pas échappé. Les manipulations de l'information, qui contribuent à miner la confiance dans les institutions et processus démocratiques, incarnent tout particulièrement cette évolution. Ce concept permet d'appréhender une ingérence étrangère menée sur le terrain informationnel, définie selon trois critères cumulatifs : une action coordonnée, permettant la diffusion massive de nouvelles fausses ou sciemment déformées, avec l'intention politique de nuire[1].

Face à ces menaces, la France cherche dès lors à créer les conditions d'une résilience collective. Cette résilience s'appuie notamment sur des moyens d'action (détection, saisie des autorités compétentes, poursuites

éventuelles) concertés et déployés par des administrations régaliennes (ministères des Armées, des Affaires étrangères, de l'Intérieur…), sans que ceux-ci aient pour autant valeur de doctrine. Elle repose enfin et surtout sur l'implication et le dynamisme de la société civile, que l'État cherche à encourager et à soutenir de manière continue.

L'information, terrain historique d'influences étrangères

L'espace informationnel, qui constitue un vecteur d'ingérence idéal pour tout acteur souhaitant exercer une influence politique dans un pays tiers, est notamment devenu un enjeu stratégique majeur au cours du siècle dernier. Ceci vaut en particulier pour les États démocratiques, au sein desquels l'accès à une information pluraliste, ouverte et largement diffusée peut faciliter les tentatives d'immixtion étrangères.

La France et la guerre de l'information au XXe siècle

Alors que l'information de masse apportée par la presse écrite avait pu créer les conditions d'une propagande à grande échelle tout au long du XXe siècle, la guerre de l'information n'a pris pleinement son sens qu'après la Seconde Guerre mondiale et l'entrée dans la guerre froide. La France n'échappait pas à la logique des deux blocs. Son champ informationnel devenait ainsi le terrain d'affrontement de deux visions du monde radicalement opposées. L'État, préoccupé notamment par l'antiaméricanisme et surtout l'anticolonialisme du Parti communiste français (PCF), chercha d'abord à lutter contre ce qu'il considérait comme « la cinquième colonne », suspectée d'agir au bénéfice direct de Moscou.

Le contrôle étroit exercé par le ministère de l'Information durant cette période limitait de fait l'accès des réseaux et relais communistes à la radio, et encourageait une forme d'autocensure de la majorité de la presse nationale qui relayait alors essentiellement les vues gouvernementales[2].

Par la suite, la fin des années 1970 et les élections présidentielles de 1981 constituèrent un moment de tension particulier dans le champ médiatique français ; les relais de Washington se faisaient l'écho de ses préoccupations face à l'eurocommunisme puis l'Union de la gauche, tandis que le PCF, revenu dans le giron soviétique à partir de 1977, accusait l'audiovisuel public de partialité durant la campagne. Cette tension s'est ensuite atténuée, à la suite du déclin du PCF puis de la chute de l'URSS. La domination de l'hyperpuissance américaine lors de la décennie 1990 venait entériner l'américanisation progressive de l'information, et la plus grande uniformité idéologique qui en a résulté pouvait ainsi apparaître comme un signe supplémentaire de « la fin de l'Histoire[3] ».

Les « Macron Leaks » ou l'entrée dans l'ère des manipulations de l'information

Le développement d'Internet puis des réseaux sociaux a ensuite accéléré considérablement la diffusion et le partage de l'information, entraînant de nouveaux usages et donc de nouveaux risques. La polarisation croissante des opinions se trouve notamment aggravée par la propagation de fausses nouvelles, voire de manipulations, tandis que les médias traditionnels et leur rôle de contre-pouvoir se voient profondément remis en cause. Si ces phénomènes se sont imposés progressivement au sein du débat public français, un point de bascule est cependant venu accélérer la prise de conscience étatique de ces enjeux. En mai 2017, l'élection présidentielle est entachée par l'affaire des « Macron Leaks » ; la France se trouve confrontée pour la première fois de son histoire à une campagne de manipulation de

l’information visant à déstabiliser le cœur du processus démocratique de la V^e^ République.

C’est principalement cet événement qui, à la lumière de ce qui s’était par ailleurs produit lors des élections américaines de 2016, a conduit les autorités françaises à s’interroger sur la nouvelle tournure que pouvait prendre la guerre de l’information au XXI^e^ siècle, et ainsi à caractériser le phénomène des manipulations de l’information. Ce concept, dans sa dimension exogène (des manipulations endogènes étant également envisageables[4]) désigne des phénomènes qui ont jusqu’à présent essentiellement touché des démocraties libérales occidentales, mais qui ont néanmoins pu affecter également certains pays africains et asiatiques[5].

Une réponse étatique en deux volets

Confrontée à cette tentative de déstabilisation, la France a pris conscience du caractère nouveau de ce phénomène, et des risques que celui-ci faisait peser sur ses institutions. Une première étape, conduite à l’initiative d’une partie de la communauté de recherche stratégique française, a consisté à analyser et à caractériser la menace[6]. Cette appréhension préalable a ensuite incité l’État à se doter de nouveaux moyens pour lutter contre ces tentatives de manipulation, mais aussi renforcer la résilience de la société française. Cette réponse se décline en deux volets principaux : le premier, d’ordre régalien, vise à renforcer les capacités et les moyens d’action étatiques contre les menaces ; le second, législatif, a pour ambition de proposer un cadre légal protecteur et dissuasif face aux tentatives de manipulations en période électorale.

Le niveau régalien : vigilance renforcée à l'égard des menaces et coordination en cours

Ce premier volet est conduit par les administrations des ministères régaliens, chargées de coordonner la réponse à d'éventuelles actions hostiles de la part d'acteurs étrangers dans le champ informationnel. À ce jour, il n'existe pas à proprement parler de doctrine de lutte contre les manipulations de l'information. Néanmoins, le développement d'une appréhension stratégique commune du phénomène pourrait amener l'État à se doter de capacités pour y faire face. Les ministères de l'Europe et des Affaires étrangères, des Armées, de l'Intérieur et de la Justice se sont ainsi saisis de la question, en lien avec les services du Premier ministre. Ces premières concertations sont susceptibles d'être étendues à d'autres acteurs étatiques et de dégager les grandes lignes d'une potentielle stratégie de lutte contre les manipulations de l'information. Des arbitrages à l'échelle interministérielle pourraient donner lieu par la suite à la création d'une structure ou d'une équipe dédiée au traitement de ces sujets.

Cette action se traduit jusqu'à présent par des exercices de simulation de crise, mais aussi par des dispositifs de veille stratégique effectuée sur les réseaux sociaux et les principaux médias français et étrangers, afin de déceler les grandes tendances à l'œuvre dans le champ informationnel et d'attirer l'attention sur le traitement de certains enjeux ayant directement trait aux intérêts français. Cette étape, essentielle pour repérer en amont des discours de fond qui peuvent par la suite resurgir lors de campagnes ultérieures, relève davantage d'un moyen de défense passive. La détection (de plus en plus automatisée) et la qualification (phase d'analyse permettant de qualifier la nature de l'attaque) des manipulations de l'information nécessitent cependant d'autres outils, dont le ministère de l'Europe et des Affaires étrangères a notamment initié le développement. Par ailleurs, ces différentes administrations conduisent également un dialogue continu avec les plateformes technologiques, qui constituent aujourd'hui l'un des

vecteurs principaux de la circulation de l'information, afin de les inciter à davantage d'ouverture et de transparence, ainsi qu'à mieux prendre en compte le caractère éminemment évolutif du champ informationnel.

Le niveau législatif : une prévention des risques électoraux

Le second volet de la réponse est de nature législative. La proposition de loi relative à la manipulation de l'information, adoptée en novembre 2018, est venue renforcer l'arsenal à disposition de l'État français pour lutter contre les tentatives de déstabilisation étrangères en période électorale. Applicable au cours des trois mois précédant les scrutins à enjeux nationaux – élections présidentielles, législatives, sénatoriales, européennes et référendaires – et jusqu'à date de ceux-ci, elle induit des obligations de coopération et de transparence accrues pour les plateformes numériques, concernant aussi bien la nature de leurs algorithmes que les contenus qu'elles peuvent héberger (publicités politiques au premier chef). La loi permet par ailleurs la saisine d'un juge des référés pour statuer sous 48 heures de la qualification de l'information suspectée et ordonner la cessation de sa diffusion auprès des acteurs concernés (hébergeurs, plateformes, fournisseurs d'accès)[7]. Enfin, elle renforce les pouvoirs du Conseil supérieur de l'audiovisuel (CSA) en termes d'encadrement du paysage audiovisuel français.

Cette loi a cependant engendré des controverses. Elle a pu être perçue comme un moyen de renforcer le contrôle étatique sur l'espace informationnel et *a fortiori* de limiter la liberté de la presse, perception notamment renforcée par la création concomitante – annoncée lors de la deuxième lecture de la loi – du Conseil de déontologie journalistique et de médiation, instance d'autorégulation de la profession soutenue par le gouvernement. Plus encore, elle a fait naître la crainte que les plateformes

anticipent d'éventuelles sanctions en censurant systématiquement les contenus jugés suspects, par volonté de se conformer au droit[8].

Une co-construction de la résilience de la société française

La résilience du corps social français s'est notamment manifestée lors des « Macron Leaks », les fausses informations à caractère personnel qui ont été divulguées n'ayant pas atteint leur objectif de déstabilisation. Cette résilience s'explique en partie par certaines caractéristiques du scrutin présidentiel français. Le suffrage direct à deux tours rend les pronostics plus complexes, et la législation stricte en matière de publicité électorale[9] ne permet pas les mêmes dérives que dans un pays comme les États-Unis. Mais d'autres facteurs propres à la culture politique française ont certainement joué un rôle majeur : l'environnement médiatique pluraliste, professionnel et moins polarisé que son équivalent américain ; une population qui dispose d'un niveau d'éducation aux médias relativement élevé et dont le développement de l'esprit critique est encouragé au cours du parcours scolaire.

Une sensibilisation croissante de la société

La propension des médias français à s'organiser pour apporter leur propre réponse à la diffusion de fausses informations, intentionnelles ou non, joue également un rôle certain dans le renforcement des anticorps de la société face aux menaces informationnelles. La multiplication des services de vérification des faits (*fact-checking*) au sein des rédactions[10] et l'augmentation des moyens qui leur sont alloués constituent des remparts

supplémentaires contre des tentatives de manipuler l'opinion publique. Ces dispositifs sont par ailleurs un moyen de renouer avec les franges les plus sceptiques du lectorat et de restaurer une partie de la confiance perdue auprès de l'opinion. Or cette confiance est essentielle pour promouvoir un environnement informationnel susceptible de favoriser des réactions adéquates face aux ingérences étrangères.

À ce titre, il faut rappeler que de nombreuses initiatives d'éducation aux médias, personnelles, collectives et institutionnelles[11] ont émergé au cours des dernières années et contribuent elles aussi à la résilience du corps social, en particulier en milieu scolaire. L'éducation aux médias et à l'information (EMI) fait désormais partie des cursus de primaire et de secondaire, à travers l'enseignement moral et civique[12]. Le Centre pour l'éducation aux médias et à l'information, notamment chargé de l'organisation de la « Semaine de la presse et des médias dans l'école », contribue à la sensibilisation des jeunes publics à la complexité du champ informationnel. Soutenus par les ministères de la Culture et de l'Éducation, ces dispositifs constituent un atout supplémentaire pour faire face aux tentatives de manipulation de l'information. Reste qu'ils gagneraient probablement à être étendus à l'ensemble des classes d'âge de la population française, au regard du rapport potentiellement problématique que certains seniors peuvent entretenir avec l'information dans l'espace numérique[13].

Initiatives partagées et multi-acteurs

En plus de sa propre action de lutte contre les manipulations de l'information, l'État français considère que le développement de capacités de résilience collective incombe en premier lieu à la société civile. Soucieux de ne pas apparaître comme l'arbitre d'une vérité absolue, il ne jouerait qu'un rôle d'appui et de soutien. Dès lors, l'enjeu est de parvenir à co-construire avec cette dernière une politique à même de renforcer

durablement ces capacités. Cette logique s'incarne notamment au travers de deux initiatives respectivement soutenues et menées par le ministère de l'Europe et des Affaires étrangères.

La première est le Partenariat international pour l'information et la démocratie, impulsé par les travaux de l'ONG Reporters sans frontières sur l'élaboration par des pairs de critères pour statuer sur la fiabilité et la qualité d'une information[14]. Soutenu initialement par onze États sollicités par la France, rapidement rejoints par une vingtaine d'autres, ce partenariat incite les États et les grands acteurs de presse à promouvoir les libertés d'opinion et d'expression, ainsi que l'accès à une information libre, pluraliste et fiable. Il invite également les entreprises structurant l'espace de l'information à faire preuve de transparence, responsabilité et neutralité dans leurs pratiques de diffusion de l'information.

La seconde initiative s'est structurée à partir d'une non-conférence – un événement participatif conduit sous la forme d'ateliers, au cours duquel les participants contribuent directement à l'élaboration de solutions aux enjeux examinés – organisée au Quai d'Orsay, réunissant divers acteurs luttant contre la désinformation (développeurs, chercheurs, activistes…). À l'appui de la communauté de recherche et d'experts techniques, cet événement a notamment permis de développer des outils en source ouverte « pour renforcer les anticorps de la démocratie déjà présents dans nos sociétés[15] », ainsi que d'élaborer un recueil de bonnes pratiques en matière de lutte contre les manipulations de l'information. Accessibles à tous, ces éléments participent d'une volonté de mettre à disposition de la société des instruments nécessaires à sa participation active dans la lutte contre les menaces informationnelles.

Pour aller plus loin

JEANGÈNE VILMER Jean-Baptiste, ESCORCIA Alexandre, GUILLAUME Marine, HERRERA Janaina, *Les Manipulations de l'information : un défi pour nos démocraties*, rapport du Centre d'analyse, de prévision et de stratégie (CAPS) du ministère de l'Europe et des Affaires étrangères et de l'Institut de recherche stratégique de l'École militaire (IRSEM) du ministère des Armées, Paris, août 2018.

JEANGÈNE VILMER Jean-Baptiste, *The « Macron Leaks » Operation : A Post-Mortem*, Atlantic Council & IRSEM Report, juin 2019.

MOURON Philippe, « Du Sénat au Conseil constitutionnel : adoption des lois de lutte contre la manipulation de l'information », *Revue européenne des médias et du numérique*, IREC, juin 2019, p. 9-11.

PÉTINIAUD Louis et LIMONIER Kevin, « Cartographier le cyberespace : le cas des actions informationnelles russes en France », *Les Champs de Mars*, 2018, n° 30, vol. 2, p. 317-326.

TAILLAT Stéphane, CATTARUZZA Amaël et DANET Didier (dir.), *La Cyberdéfense. Politique de l'espace numérique*, Paris, Armand Colin, 2018.

VENINGER Guy, « Ingérence numérique, mode d'emploi », *Le Débat*, 2020, vol. 208, n° 1, p. 42-55.

IV

LES RÉPONSES SCIENTIFIQUES, JURIDIQUES ET POLITIQUES

CHAPITRE 14

Les enjeux de la réception : comment mesurer l'influence de la désinformation ?

Divina Frau-Meigs

Les fausses informations, encore appelées infox, s'avèrent être des armes d'influence en temps de paix. La plupart des acteurs de tous les secteurs (politique, défense, éducation…) ont sous-estimé l'impact des plateformes de médias sociaux dans la fabrique et le relais de l'influence. Le secteur de la recherche n'est pas en reste, car il se focalise sur les usages commerciaux et les risques personnels plutôt que sur les risques démocratiques. De fait, alors que le phénomène a commencé en 2012 avec l'élection d'Obama, les recherches n'ont vraiment débuté qu'en 2016 aux États-Unis et accusent encore un retard certain en Europe. D'où le biais intrinsèque de beaucoup de travaux actuels, qui viennent des États-Unis et transposent les résultats américains à l'Europe, alors que les publics et les situations sont différents. Il se justifie toutefois par le caractère mondialisé du phénomène de l'infox, avec son « effet transverse » : transfrontière, translangue, transmédia[1].

En France, les sciences politiques et les sciences de l'information-communication sont aux avant-postes de la recherche sur la désinformation. Toutefois, elles ont mis du temps à se préoccuper de la mesure de l'influence car elles sont dominées par l'école des usages, qui tend à minimiser les effets des médias pour mettre en avant les capacités immuno-protectrices des pratiques des internautes. La question de l'influence revient toutefois sur le devant de la scène car la désinformation vise à manipuler l'opinion et, en conséquence, à agir sur les prises de décision des citoyens, particulièrement en période d'élections.

L'influence associe des phénomènes de pouvoir ne reposant pas sur une autorité légale ou politique. Les médias de masse, tout comme les médias sociaux, se trouvent en première ligne en tant que façonneurs de l'opinion, exerçant une certaine emprise sur le pouvoir de penser et d'agir des citoyens[2]. L'influence ne peut être dissociée des mécanismes de ciblage et des procédés de diffusion, très importants dans le cadre des activités de désinformation. Les implications de cette forme de conflictualité tiennent dans l'efficacité de l'impact en réception et dans les solutions possibles du côté de la résilience des usagers, notamment des citoyens lors des périodes de vulnérabilité que sont les élections. Des résultats de la recherche dépendent en effet un certain nombre d'actions possibles : légiférer, fiscaliser, censurer, éduquer…

La littérature fait apparaître deux gros corpus de recherches empiriques : un corpus assez homogène focalisé sur les élections ; un corpus plus hétérogène portant sur le régime médian de la désinformation (hors élections). Les questions de recherche sur les élections s'intéressent à la fabrique de l'opinion, notamment la polarisation potentielle des publics conçus comme des électeurs (et des citoyens). Les questions de recherche sur le régime médian s'attachent à la manipulation des publics, notamment par les biais cognitifs et les dispositifs socio-techniques qui sont vecteurs de l'influence (bulles de filtre, chambres d'écho, algorithmes, chatbots).

Dans les deux cas, outre l'attention portée aux donneurs d'ordres, en amont de l'infox, les recherches entérinent l'agentivité de certains usagers en aval : ceux-ci ne sont pas des récepteurs passifs des messages, mais des agents actifs de leur amplification. C'est ce que souligne la définition de la désinformation fournie par le groupe d'experts sur la désinformation de l'UE : « Information porteuse de risque de danger à l'information, qui touche tous les secteurs, poussée par la production de désinformation à des fins de gains économiques, politiques ou idéologiques, exacerbée par la façon dont les audiences et les communautés s'impliquent et amplifient la désinformation[3]. » La désinformation à l'ère numérique constitue un phénomène spécifique et nouveau en raison précisément de cette navette permanente entre producteurs et récepteurs et entre médias de masse et médias sociaux.

Caractériser les mécanismes de la désinformation

La désinformation se mesure en termes de polarisation des publics conçus comme des électeurs et des citoyens. Elle fait l'objet de beaucoup de littérature grise (rapports, enquêtes, auto-saisines…) et pas seulement de recherche fondamentale, ce qui marque l'urgence du sujet et une mobilisation multi-acteurs face à un déficit de connaissances[4].

La polarisation des publics et l'exposition sélective

Les recherches menées aux États-Unis tendent à se focaliser sur les élections présidentielles de 2016, pour essayer de savoir si la désinformation a pu influer sur un scrutin aux résultats quelque peu inattendus. En termes de réception et d'impact, elles pointent toutes une

« polarisation asymétrique » entre les candidats et une « exposition sélective » à la désinformation selon des lignes partisanes, les électeurs pro-Trump étant beaucoup plus susceptibles de visiter des sites d'infox que les pro-Clinton[5]. Elles concluent que les Américains ont tendance à croire les mises en récit en faveur de leur candidat, surtout s'ils suivent des médias sociaux répartis idéologiquement[6]. En général, la consommation de désinformation tend à servir de complément plutôt que de substitut à l'information avérée : les visiteurs de sites de *fake news* sont parmi les plus gros consommateurs d'actualités et ceci ne baisse pas notablement pour les individus les plus politiquement avisés[7].

Les recherches en France se concentrent sur les élections présidentielles de 2017 pour savoir si les infox ont eu une influence sur la campagne. Elles montrent que la portée des sites de désinformation en lien avec la population en ligne est très faible (1 % en France par contraste avec le site du *Figaro* dont la moyenne mensuelle est de 22,3 %). En outre, le niveau des interactions sur Facebook (nombre de clics, de commentaires, de partages et de réactions) est généré par un petit nombre de sites de désinformation et reste très inférieur à celui produit par les médias de référence en matière d'actualités. Les médias soutenus par le gouvernement russe, comme Russia Today (RT) et Sputnik, s'avèrent être aussi de portée limitée, de même que l'engagement et le nombre d'interactions qu'ils occasionnent, par contraste avec les sites de médias nationaux établis[8].

Les premiers travaux français qui se sont aussi penchés sur l'exposition sélective et sur la polarisation aux extrêmes notent la faible présence d'infox pendant la campagne. Ils soulignent le rôle des communautés politiques dans sa mise en circulation et indiquent aussi que les fausses informations tendent à être cantonnées à leur communauté, se propageant localement, ce qui confirmerait un effet de chambre d'écho, à savoir l'affichage d'une sélection homogène de points de vue au sein du collectif[9]. Ils font aussi apparaître des différences de comportement entre

communautés en ligne, selon leur proximité avec un candidat : les partisans de Marine Le Pen et François Asselineau sont ceux qui, en moyenne, ont partagé le plus de liens vers des sources considérées comme peu fiables dans la base du Décodex du *Monde*. Les contenus sont distribués de manière différente par différentes communautés politiques, révélant une polarisation liée à l'appartenance partisane, avec une audience très restreinte[10].

La propagation locale des discours radicalisés

Des travaux plus récents, en 2019, ont évalué le rôle de l'écosystème des médias de masse et des médias sociaux dans la polarisation, en comparant la France et les États-Unis. Ils révèlent une polarisation américaine sur l'axe horizontal droite/gauche, en fort contraste avec la France, où la polarisation se place sur un axe vertical élites institutionnelles/anti-élites. Les médias traditionnels forment un « cœur » regroupant des médias de gauche et de la droite modérée. Ils se trouvent confrontés à de nouveaux médias « politisés » et « partisans », unis par le rejet des élites (comme par exemple Les Crises, Égalité et Réconciliation, Fdesouche, Sputnik, etc.)[11].

L'apparition de ces médias contestataires alerte sur quatre facteurs d'évolution majeurs entre médias sociaux et médias de masse : les effets de réseau qui font que les deux secteurs s'entre-citent ; l'émergence de nouveaux médias fortement politisés à droite qui ont gagné rapidement en audience et en influence (comme par exemple Russia Today, Fdesouche, Sputnik, etc.) ; les liens entre ces médias et des médias satellites (Français de France, Presse Galactique, WikiStrike, Stop Mensonges) qui s'entre-citent ; et enfin des figures polarisantes de polémistes qui agissent comme des agents « blanchisseurs » lorsqu'ils mettent en avant de la désinformation produite par ces médias[12].

La recherche reste donc prudente sur les effets directs de la désinformation politique, notamment en lien avec l'intégrité des élections (à la fois leur bon déroulement et la légitimité de leurs résultats). Elle semble renforcer l'opinion des plus convaincus et des plus radicalisés aux extrêmes, qui restent une minorité. Celle-ci est réactive à la présentation orientée de l'information (en laquelle elle croit déjà) et tend à l'amplifier et la viraliser, utilisant alors l'effet de chambre d'écho qui s'avère important dans ce cas précis seulement, pour alimenter des communautés partisanes locales. Toutefois, celles-ci ont tendance à une amplification d'opinions négatives et peuvent affecter le système de vote, en réduisant les points de discussion du débat public.

La systématisation des attaques

En période pré-électorale et électorale, les sentinelles traditionnelles, que ce soient les médias de référence ou les ONG de la société civile, exercent une surveillance continue. Hors de cette période, c'est-à-dire en régime médian, la désinformation est généralement étudiée en lien avec les « menaces hybrides ». Celles-ci sont définies par l'UE dans son Plan d'action contre la désinformation comme « le mélange d'activités coercitives et subversives, de méthodes conventionnelles et non conventionnelles […] susceptibles d'être utilisées de façon coordonnée par des acteurs étatiques et non étatiques […] sans que le seuil d'une guerre déclarée officiellement soit dépassé[13] ». Ces fausses nouvelles sont plus directement associées à la propagande classique, augmentée par les usages et outils numériques, en temps de paix, où l'infox devient une arme de manipulation massive.

Ces travaux, notamment issus de la task force East Stratcom, se focalisent sur les campagnes de désinformation de la Russie et tendent à considérer les pays limitrophes de l'UE et de l'espace post-soviétique[14]. Par

contraste avec les travaux sur la polarisation en époque électorale, ils se concentrent moins sur les structures de l'influence que sur les méthodes utilisées pour influencer. Ils soulignent le recrutement d'acteurs parmi les publics actifs agissant par procuration pour fabriquer et amplifier un contenu idéologique, fortement populiste. Ils notent ainsi que dans les pays Baltes, 10 % des usagers actifs diffusent et relaient près de 70 % des contenus sur le réseau social russe Vkontakte (équivalent de Facebook)[15].

Ces travaux tendent à montrer un temps long de l'influence (avec implantation antérieure, en amont de la période d'élections ou de campagnes). Ils considèrent l'influence comme une pièce de l'arsenal de la cyberguerre de l'information, en mettant en avant la notion de « campagnes de désinformation » où les réseaux sociaux font l'objet d'une « utilisation quasi militaire » (*weaponization*) à des fins de déstabilisation. Centrés sur les communautés minoritaires dans les pays post-communistes, ils font apparaître l'émergence de trolls, à savoir des personnes qui visent à générer des polémiques en s'infiltrant dans des communautés en ligne, et signalent l'importance des mèmes, ces petits éléments visuels ou sonores comme des GIF, propagés de manière récurrente et virale par hyperlien ou hashtag. Ils font partie d'un dispositif prêt-à-amplifier, avec la possibilité de créer des récits qui dévalorisent et dénigrent l'ennemi, souvent en ayant recours à des cadrages pro-Russie[16]. L'activité concertée et coordonnée des trolls pour influencer les audiences se déroule en trois phases : « poser l'appât, déployer le filet et ramener la prise » (*luring, taking the bait and hauling in*)[17].

En termes de rhétorique, l'analyse du langage des trolls et des mèmes fait apparaître des constantes, adaptées selon les pays visés et leurs langues : l'opposition « nous *vs* les autres », les métaphores nationales détournées, les néologismes accrocheurs, et le recours aux stéréotypes. La manipulation des images, plus susceptible d'engager l'émotion des internautes, est associée à des commentaires décontextualisés, des dates

modifiées ou des lieux déplacés. Sont ainsi mises en évidence les stratégies principales du côté de la Russie : appel à la nostalgie (c'était mieux avant), dénonciation de l'oppression des minorités russophones (dans les pays post-communistes), corruption des instances dites démocratiques et fait religieux (en amalgame avec ladite « crise » des migrants). Et ce, dans un cadrage où le recours à une « grande Russie » pacifiste, victime d'une phobie antirusse, et ne répondant pas aux provocations de l'Ouest apparaît comme le seul rempart [18].

Une méthode de l'influence ressort particulièrement : la construction de cadres repérables et prêts à l'emploi, l'organisation de conversations en ligne par le biais de sites et influenceurs reconnus, le recours à des mèmes visuels qui créent une empreinte durable, consciente et inconsciente, chez les usagers. Ces travaux font apparaître le montage de récits bien calibrés, avec d'autres mécanismes en appui, comme les fuites massives de documents, y compris de documents falsifiés. La présence de minorités est un élément de fragilisation, surtout si l'amalgame peut être fait avec les migrants, dans des mises en récit de risque de déplacement et de nostalgie patriotique qui viennent se mettre en résonance objective avec des éléments extrémistes partageant les mêmes récits dans les pays cibles.

Analyser les vecteurs de diffusion des infox

Concernant les vecteurs d'influence, les chercheurs s'intéressent moins à démontrer le « comment » qu'à comprendre le « pourquoi ». Certains analysent l'influence des plateformes numériques – par sélection algorithmique ; d'autres tentent de démontrer l'influence des humains – par exposition sélective. Les recherches portent à la fois sur les biais cognitifs et sur les dispositifs socio-techniques des vecteurs de l'influence : se pose la question des algorithmes et des chatbots, ces petits programmes pilotés par

l'intelligence artificielle qui peuvent tenir des conversations comme des humains, mais aussi du rôle des chambres d'écho qui proposent une sélection homogène de points de vue à une communauté donnée et des bulles de filtre, ces offres personnalisées qui confortent les usagers dans leur point de vue et qui pourraient créer un « déterminisme de l'information » selon lequel nos opinions dans le passé régissent notre accès à toute nouvelle information[19]. Ces travaux font apparaître des causes liées à la nature humaine (biais ou failles cognitives, fracture numérique, manque d'éducation et de connaissances…) et des causes sociétales, liées à l'évolution de l'espace public et du collectif à l'ère numérique (déplacement des institutions, perte de monopole de l'État-providence, crise des médias…).

L'influence pilotée par les algorithmes : chambres d'écho et bulles de filtre

Des chercheurs se sont intéressés à la maximisation algorithmique de l'influence, par le biais des chambres d'écho notamment, en soulignant leur tendance à l'homophilie, même lorsque la désinformation n'est pas l'objectif à l'œuvre, en régime médian[20]. Les travaux de Quattriocchi comparent des chambres d'écho pro-science et pro-complotisme sur Facebook. Dans les deux cas, elles tendent à promouvoir leur point de vue préféré, en des cascades de posts au sein des deux communautés. Cette agrégation d'informations préférées renforce l'exposition sélective et la polarisation : les usagers ont tendance à commenter et à disséminer seulement les éléments qui confirment leur théorie et à ignorer les réfutations. De fait, les croyances complotistes sont plutôt renforcées après réfutation : le petit groupe qui interagit après la réfutation augmente son activité dans la chambre d'écho[21]. Cela se répercute aussi sur l'expression des émotions, qui tend à être de plus en plus négative à mesure que les

individus restent plus longtemps dans la chambre d'écho. Plus un usager polarisé est actif, plus il produit des commentaires à valeur négative, que ce soit pour le groupe pro-science ou le groupe pro-complotisme[22].

Ces résultats suggèrent que l'effet de chambre d'écho est un phénomène restreint mais profond. De même pour le phénomène des bulles de filtre, où c'est l'appartenance partisane des internautes qui crée l'exposition sélective[23] : les identités et identifications politiques sont plus fortes que les algorithmes de recommandation. D'une certaine manière, les motivations idéologiques fonctionnent comme une forme de traitement de l'information qui promeut les intérêts des individus et les aide à faire le tri des nouvelles et à conforter leurs croyances en lien avec leur loyauté au groupe d'appartenance affinitaire[24].

D'autres chercheurs encore associent les bulles de filtre à l'analyse de sentiments pour essayer de comprendre comment les fausses croyances émergent et informent les internautes, voire suscitent une contagion des émotions[25]. Deux émotions, la colère et l'anxiété, semblent déterminer en partie la façon dont les citoyens considèrent l'information, soit en mode partisan/clos, soit en mode non-partisan/ouvert. La colère encourage le mode partisan et motive une évaluation de l'information qui conforte la croyance dans le parti politique soutenu. Au contraire, l'anxiété agirait en amont, pour initier des croyances qui sont moins fondées sur le mode partisan que sur l'environnement informationnel. Colère et anxiété peuvent donc affecter l'exactitude des croyances politiques en renforçant ou en atténuant l'influence de l'idéologie[26].

En outre, ces émotions sont contagieuses et peuvent se répandre sur les réseaux sociaux comme Facebook. Les états émotionnels pourraient se transférer entre internautes, sans que ces derniers en soient aussi conscients que lorsque les interactions sont directes entre pairs ou entre amis. Cela peut renforcer la motivation à divulguer et à amplifier des *fake news*

d'individus attachés aux croyances qui renforcent leur identité et leur centralité, notamment en matière de réputation et d'influence[27].

Ces résultats réduisent la portée des chambres d'écho et des bulles de filtre, tout en confirmant leur existence substantielle dans l'attachement aux fausses croyances[28]. Ces affichages sélectifs semblent fonctionner pour un sous-groupe réduit d'internautes parmi les plus convaincus et les plus actifs, c'est-à-dire pour des personnes susceptibles de visiter des sites de désinformation de manière disproportionnée par rapport à la population générale[29]. Ils peuvent dans ce cas renforcer les préférences des internautes *via* leurs algorithmes de personnalisation (fondés sur l'historique de navigation et la géolocalisation), et ainsi contribuer à la réduction de la visibilité de contenus nuancés au profit des contenus polarisés[30].

L'influence pilotée par les humains : biais cognitifs et influence continue

D'autres éléments explicatifs sont fournis pour décoder l'influence des fausses informations. Aux émotions que sont la colère et l'anxiété, certains chercheurs ajoutent deux valeurs de l'information en tant que telle : la nouveauté et la surprise (qui peuvent ensuite déclencher colère ou anxiété). Cet engouement pour les nouvelles sensationnelles peut expliquer que les fausses informations se propagent plus vite que les vraies car elles suscitent le besoin de partage. Ces émotions affectent à leur tour la préférence sélective et la polarisation[31]. Ce biais en faveur de la nouveauté favorise l'amplification des infox, qui suscitent plus d'intérêt (sinon de croyance ou d'adhésion) et qui enclenchent d'autres mécanismes sociétaux, comme les enjeux de réputation, de statut social, d'influence[32]. Leur rhétorique spectaculaire, voire alarmiste, peut jouer sur l'anxiété et la colère et enclencher nos biais cognitifs. Elle relève ici moins de la propagande que de la publicité, qui utilise aussi les neuro-sciences en neuro-marketing pour

attirer l'attention, et ce encore plus sur les médias sociaux qui recherchent l'engagement des usagers.

Les biais cognitifs sont enclenchés comme un mécanisme de tri, face au trop-plein d'informations à traiter du fait de l'usage combiné des médias de masse et des médias sociaux[33]. Ils créent des raccourcis rapides, qui peuvent sembler irrationnels parce qu'ils se fondent sur des faits erronés, non établis, mais toutefois plausibles. Ils s'appuient sur un mélange de préférences personnelles et d'attentes sociales. C'est leur plausibilité qui fait que l'activation des mécanismes de vérification des sources se trouve inhibée. La désinformation est d'autant plus efficace que la fausse information véhiculée est conforme aux points de vue politiques, religieux ou sociaux préexistants[34].

La compilation des recherches sur la désinformation fait apparaître un certain nombre de biais saillants et récurrents, en particulier le biais de confirmation, le biais d'autorité, le biais de disponibilité en mémoire et le biais d'attribution[35]. Stephan Lewandowsky pointe en particulier le biais d'influence continue : l'infox est plausible avec le système de croyance ou l'idéologie des individus et réclame moins d'effort cognitif[36]. Il identifie ce biais comme étant celui où les individus refusent de croire les arguments de la réfutation, et au contraire se trouvent doublement confortés dans leur jugement : si les autres mettent tellement d'efforts à réfuter, c'est qu'il y a, suivant l'adage, « anguille sous roche » et qu'il n'existe « pas de fumée sans feu ».

Ces biais se retrouvent aussi dans les travaux sur le conspirationnisme, qui fait partie de la sphère de la désinformation. Ils relèvent de la tendance exagérée à croire que tout effet est causé par une action intentionnelle, qui peut bénéficier à un groupe privilégié d'initiés. Le conspirationnisme fait aussi appel à des communautés en chambre d'écho, avec une ultra-minorité très active, voire prête à passer à l'action de manière radicale ou extrême, avec des effets déstabilisateurs. Polarisation et radicalisation vont alors de

pair. La plupart des conspirationnistes utilisent des arguments qui en apparence sont rationnels, mais qui manquent de fondements scientifiques. Ils s'appuient sur des sources de leur propre fabrication, qu'ils alimentent dans leurs propres communautés sur le même modèle que les communautés scientifiques, leur donnant un semblant de cohérence[37]. Leurs procédés rhétoriques sont proches de ceux de la propagande et des cybermenaces, en ce qu'ils inversent la charge de la preuve (« prouvez-nous que nous avons tort »), qu'ils avancent des opinions difficiles à réfuter et qu'ils alimentent l'idée d'une machination secrète derrière tout événement[38].

La crise épistémique née de la défiance généralisée

D'autres chercheurs enfin attribuent la cause profonde du problème de la désinformation à des facteurs externes au fonctionnement des médias de masse et des médias sociaux, eux-mêmes en crise. Leurs travaux relèvent plutôt de réflexions philosophiques ou sociologiques. Pour eux, la montée de l'opinion face à l'information révèle une crise épistémique, dont une des retombées est de relativiser la vérité et son interprétation, d'où son association à la notion de « post-vérité[39] ».

C'est dans cette pauvreté des connaissances que viennent s'engouffrer des infox du type négationnisme, révisionnisme historique, conspirationnisme, *via* des formats médiatiques pseudo-informatifs comme le recours aux chroniqueurs ou aux influenceurs qui peuvent être confondus avec des journalistes, mais qui n'en sont pas. Ce type de *fake news* peut avoir recours à toutes sortes de pseudo-sciences, avec revues et sites Web à la clé, voire monter des universités sur YouTube comme UPrager. Elles légitiment la manipulation, la simplification ou le détournement d'approches scientifiques respectées comme les travaux de Michel Foucault ou encore de Jacques Derrida, en gommant toutes les précautions prises par

ces chercheurs pour montrer la vérité comme une construction sociale et la recherche comme une série de controverses fructueuses.

La croyance aux *fake news* est alors aussi liée au bas niveau d'éducation de la population concernée, au-delà de l'attachement partisan et des biais cognitifs[40]. Par ailleurs, les individus les plus touchés sont aussi susceptibles d'être les plus âgés car ils sont moins formés aux usages des médias sociaux et plus retranchés dans leurs préférences politiques[41]. Mais les rares travaux du point de vue des audiences montrent une résilience plus grande que ce qu'on aurait pu soupçonner dans le reste de la population. Si les gens considèrent la différence entre vraies et fausses nouvelles comme une différence de degré seulement, ils identifient ces dernières à un mixte de mauvais journalisme, de propagande polarisée et de publicité déguisée aux contenus sponsorisés. Ils n'incriminent pas tant leurs semblables que les personnalités politiques, ainsi que les médias de masse et les médias sociaux qui les publient et les diffusent. Ils les associent à un climat de défiance à l'égard de tous les médias et du monde politique[42].

Évaluer l'influence en désinformation

Les recherches sur la désinformation ont augmenté de manière exponentielle depuis 2016. Les chercheurs ont bénéficié d'un effet d'aubaine lié à la panique médiatique et sociale causée par le double scandale de Cambridge Analytica et d'*IRA vs United States of America*[43]. Ils ont ainsi pu booster l'usage de méthodes originales et mixtes en sciences humaines et sociales, en faisant un saut qualitatif et quantitatif vers l'usage des big data, notamment pour l'analyse de réseaux sociaux, la visualisation de données, la recherche algorithmique, les outils de linguistique appliquée, les analyses de sentiment et le *machine learning*.

Dans leur ensemble, l'évolution des travaux marque le passage d'une étape euphorique où les recherches proposées se voulaient techniques, appuyées par l'intelligence artificielle (IA) et le *big data*, à une étape sans illusion où l'analyse des facteurs humains a pris le dessus. Elle met désormais en évidence une combinatoire de deux ressorts dans la désinformation et son influence : un ressort cognitif et un ressort algorithmique. Le ressort cognitif est de loin le plus influent, qui rassemble des individus qui se ressemblent et se confortent dans leurs opinions. Le ressort algorithmique est tout aussi humain, mais avec l'aléatoire organisé de la machine : les traces de nos activités en ligne sont traitées *via* les plateformes en ligne de sorte que les médias sociaux nous influencent par l'historique de nos propres goûts et de nos valeurs.

L'étude du rôle des usagers : vers un nouveau modèle de l'influence

Les travaux confirment dans leur ensemble le rôle des médias sociaux comme potentiel d'appui à l'influence de la désinformation, avec des retombées dans la vie réelle (*In Real Life*), plutôt que comme cause directe avec un effet immédiat. Ils ont permis de comprendre des mécanismes sous-estimés, voire inédits, du côté de l'agentivité des usagers, qui sont actifs et réactifs dans la désinformation, car ils peuvent être désinformés et désinformer à leur tour. Cette inversion réciproque relève du « renversement du modèle de validation de l'information[44] ». C'est désormais l'usager qui est en position d'autorité et de responsabilité par rapport à l'information qu'il produit, retraite, mixe, diffuse et recense : il a accès à des stratégies lui permettant de contrôler toute la chaîne éditoriale de l'information, de sa production à sa mise en ligne pour diffusion.

Par conséquent, il semblerait qu'il en soit de même pour l'influence : elle aussi s'appuie sur le renversement du modèle de validation de

l’information, tournant la fabrique de l’information en fabrique de la désinformation. Cela modifie aussi le modèle de diffusion de l’information et de l’influence, avec un rôle accru de certains usagers amplificateurs qui deviennent des infomédiaires[45]. Une ébauche de typologie d’influenceurs spécifiques à l’infox se dessine à partir des différents sites et donneurs d’ordres relevés à travers diverses recherches. Elle demanderait à être développée mais permet déjà de repérer des profils hybrides : le fan/relayeur, le polémiste/humoriste, le chroniqueur/blanchisseur, le partisan/extrémiste, la taupe/troll.

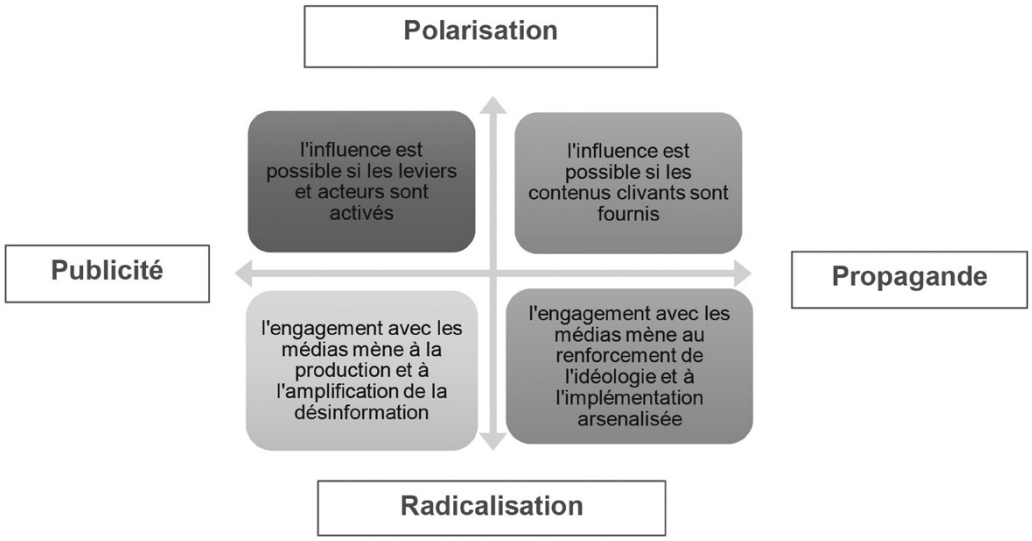
C’est dans cette inversion que se glissent et se jouent les campagnes d’influence, avec une mutation de la notion de public : de simples audiences se transforment en communautés (chambres d’écho, cascades de tweets…) où l’exposition à l’information se mêle à l’information aux autres, où les faits objectivés se juxtaposent aux faits socialisés, le tout faisant l’objet d’extractions de données et d’analyses du sentiment et de formes de l’engagement dans un réseau de pairs, qui s’amplifie par réputation et recommandation.

Attention donc aux vulnérabilités de la recommandation, qui peuvent se construire comme une forme d’influence alternative, pilotée par algorithmes. Tous les médias sociaux se sont transformés en moteurs de recherche et en sources de recommandation, affectant ainsi toute la chaîne de valeur de l’information et de l’influence. Ces machines à recommander, dont le dessein est de maintenir l’usager engagé et connecté indépendamment du contenu diffusé (YouTube), créent de véritables failles et fragilités dans le système de l’information, au profit de l’influence.

Ainsi, les effets de l’autosélection volontaire humaine et les effets de la présélection automatique par algorithmes sont moins à opposer qu’à prendre dans leur continuité et leur renforcement mutuel. Départager ce qui vient des flux sociaux générés par les algorithmes de la similarité idéologique des contacts sociaux en ligne est certes important, mais la

combinaison de ces différents éléments est cruciale à maîtriser. En somme, l'épistémologie de l'influence en désinformation qui se dégage semble pointer deux axes forts : entre publicité et propagande, d'une part, et entre polarisation et radicalisation, d'autre part (voir figure 3). Elle fournit des indications sur le rôle de l'influence et sur la probabilité de l'engagement.

Figure 3. – Épistémologie de la désinformation



Les limites de l'enquête

La plupart des recherches minimisent donc l'effet direct de la désinformation, et mettent en avant la difficulté à établir une jauge de l'influence car l'exposition ne vaut pas l'engagement ou la conviction. Celles qui notent un faible impact direct alertent sur la possibilité d'une validation implicite due au contrat de partage sur les médias sociaux, faisant jouer la pression sociale par sursaturation de l'espace public médiatique[46]. Toutefois, il n'existe pas encore une masse critique de travaux pour pouvoir se prononcer sur les effets diffus et à long terme.

Des parallèles pourraient être faits avec d'autres recherches sur les effets des médias, qui tendent à montrer que l'influence n'est pas là où l'on croit[47]. Ainsi la recherche sur les effets de la violence à la télévision montre que les cas d'imitation directe sont peu nombreux (quoique spectaculaires), mais que le sentiment de peur et d'insécurité augmente. De même pour la désinformation, où le changement de comportement lors d'un scrutin (abstention ou adhésion populiste) semble moins à redouter que le soupçon généralisé et l'érosion de la confiance dans les institutions démocratiques. Il se produit comme un effet de bord, qui change l'état global visible et ressenti du phénomène : il lui donne sans doute plus d'importance qu'il n'en a vraiment, mais il fait aussi le jeu des marchands de soupçon, avec le risque indésirable d'accroître les comportements cyniques à l'égard de l'information, voire d'accroître les discours de haine et les comportements plus extrémistes.

D'autres limites de ces recherches sont à prendre en compte, notamment l'analyse des sentiments, qui reste très textuelle. Les chercheurs n'ont pas encore la possibilité d'analyser le poids des images et les usages transmédia des récits falsifiés. Les approches quantitatives, très largement majoritaires, ne sont pas encore accompagnées d'approches qualitatives, avec entretiens et observations de groupes plus diversifiés (en matière d'âge, de genre et d'éducation notamment). L'identification des facteurs humains se doit d'être plus robuste, ce qui implique une interaction plus directe avec les usagers, à travers des entretiens, des expériences en laboratoire, voire en neuro-imagerie. Les interactions entre humains et les robots doivent également être mieux analysées. Ces travaux mettraient au jour les micro-fonctionnements qui permettent de comprendre les enchevêtrements nouveaux entre comportements humains et logiques algorithmiques.

Ces limites pointent aussi les difficultés des chercheurs à accéder aux données des médias sociaux eux-mêmes, les plateformes étant très réticentes au partage ou cherchant à contrôler les travaux en finançant elles-

mêmes certaines recherches. Ce manque d'accès crée un angle mort de la recherche, en dépit de la créativité des chercheurs pour se procurer les données manquantes. Il donne lieu à des corpus limités, sans captation *ad hoc*, avec une volumétrie réduite ou insatisfaisante, ainsi qu'une difficulté à mener des travaux longitudinaux et des collaborations internationales.

*

Mesurer la vulnérabilité ou la résilience des individus et des institutions à ces manipulations n'est pas aisé car les causes sont multifactorielles. Plus de recherches interdisciplinaires et comparatives sont nécessaires pour comprendre un phénomène par ailleurs transfrontières. L'un des risques persistants est celui de l'indépendance de la recherche publique, car les plateformes de médias sociaux, surtout Google et Facebook, les principales incriminées, s'investissent dans le financement des travaux actuels, pour se blanchir en quelque sorte. Ces travaux se doivent d'être vulgarisés pour aider les individus, non pas tant à dire ce qui est vrai et ce qui est faux, mais à comprendre qui s'adresse à eux et avec quelle intentionnalité. C'est là le rôle de l'éducation, notamment l'éducation aux médias et à l'information, dont le projet démocratique est bien de réduire la crise épistémique suscitée par la désinformation.

Pour aller plus loin (ouvrages français)

ALBERTINI Dominique et DOUCET David, *La Fachosphère. Comment l'extrême droite remporte la bataille du Net*, Paris, Flammarion, 2016.

BADOUARD Romain, *Le Désenchantement de l'Internet. Désinformation, rumeur et propagande*, Limoges, FYP Éditions, 2017.

BOYER Bertrand, *Cybertactique : conduire la guerre numérique*, Paris, Nuvis, 2014.

BRONNER Gérald, *La Démocratie des crédules*, Paris, Puf, 2013.

CAGÉ Julia, HERVÉ Nicolas, VIAUD Marie-Luce, *L'Information à tout prix*, Paris, Institut national de l'audiovisuel, 2017.

CARDON Dominique, *Culture numérique*, Paris, Presses de Sciences Po, 2019.

FRAU-MEIGS Divina, *Faut-il avoir peur des « fake news » ?*, Paris, La Documentation française, 2019.

HARBULOT Christian, *Les Fabricants d'intox. La guerre mondialisée des propagandes*, Paris, Lemieux, 2016.

HUYGHE François-Bernard, *Fake news : la grande peur*, Versailles, VA Press, 2018.

MERCIER Arnaud (dir.), *Fake news et post-vérité : 20 textes pour comprendre la menace*, The Conversation France, 2018.

REVAULT D'ALLONNES Myriam, *La Faiblesse du vrai. Ce que la post-vérité fait à notre monde commun*, Paris, Seuil, 2018.

CHAPITRE 15

Les menaces numériques en période électorale

François Delerue

Le développement et l'omniprésence des technologies de l'information et de la communication (TIC) constituent à la fois une opportunité et un danger pour nos sociétés modernes, notamment en période électorale.

La révolution numérique a contribué à revitaliser la vie démocratique de nos sociétés. Elle a offert, entre autres choses, de nouveaux vecteurs de communication à la disposition des candidats, leur permettant de diversifier leurs messages et de s'affranchir d'un certain nombre de contraintes. Dans le même temps, elle a aussi permis de développer des vecteurs de communication entre les électeurs et les candidats, donnant aux premiers la possibilité de faire entendre leurs désirs. Ainsi, la transformation numérique a favorisé des modes plus directs et plus participatifs de démocratie. Elle a aussi mis à la portée des électeurs de nouveaux moyens pour s'informer, de manière plus active que les médias traditionnels. Force est de constater, néanmoins, que malgré toutes ces nouvelles opportunités, la révolution

numérique n’a pas permis d’endiguer la crise que traversent les sociétés démocratiques en ce début de XXIe siècle.

La transformation numérique de nos sociétés et des processus électoraux s’accompagne en effet d’un certain nombre de défis et de risques pour les démocraties modernes. L’omniprésence des TIC a permis l’émergence de nouvelles menaces à l’encontre des processus électoraux qu’il est possible de classer suivant deux catégories principales : d’un côté, les menaces en matière de cybersécurité, notamment à l’encontre des candidats, des électeurs voire du processus électoral lui-même ; de l’autre, les menaces liées à l’information des électeurs et à la définition de leur choix.

Ces deux risques vont de pair dans de nombreux cas, notamment dans le cadre des élections présidentielles américaines de 2016 et françaises de 2017. Dans ces deux exemples, il y a eu à la fois des cyberopérations à l’encontre de candidats et des campagnes de manipulation de l’information visant à influencer la liberté de choix des électeurs.

L’objectif de ce chapitre n’est pas d’offrir une étude de cas exhaustive ou un panorama complet des techniques mises en œuvre pour influencer les élections par le biais des TIC, mais plutôt d’offrir une analyse et des pistes de réflexion sur ces questions, et de souligner les relations que ces différentes opérations entretiennent entre elles, que ce soit dans leur conduite ou dans leurs effets.

Les élections présidentielles américaines : un foisonnement d’opérations diverses

Les élections présidentielles américaines de 2016 et françaises de 2017 constituent deux cas d’école de menaces numériques contre des processus

électoraux, car ils offrent plusieurs exemples de menaces numériques et montrent les interactions entre elles[1].

Le 8 novembre 2016, Donald Trump était élu quarante-cinquième président des États-Unis. Les questions de cybersécurité étaient au cœur du processus électoral. Elles ne constituaient pas un objet de débat entre les candidats, mais plusieurs menaces et incidents liés à l'utilisation des nouvelles technologies ont émaillé l'élection. Premièrement, il y a eu la controverse autour de l'utilisation par Hillary Clinton, candidate du Parti démocrate, d'un serveur personnel pour envoyer des messages électroniques professionnels alors qu'elle était secrétaire d'État[2]. Deuxièmement, sont apparus des soupçons de piratage des bases de données d'électeurs dans une quarantaine d'États américains[3]. Troisièmement, ont émergé des soupçons de piratage des machines à voter électroniques dans plusieurs États[4]. Enfin, il y a eu le piratage du Parti démocrate et la fuite en ligne d'un certain nombre de données dérobées. C'est sur ce dernier cas que nous allons nous concentrer.

Entre 2015 et 2016, l'organe directeur du Parti démocrate, le Comité national démocratique (Democratic National Committee – DNC), a été la cible de différentes opérations dans le cyberespace visant à pénétrer ses réseaux et systèmes informatiques et à y dérober des données. Ces cyberopérations sont considérées comme faisant partie d'une série d'opérations visant des organisations politiques américaines dans le cadre de la campagne présidentielle de 2016[5]. La Fédération de Russie est généralement tenue pour responsable de ces cyberopérations[6]. En bref, deux agences de renseignement russes sont considérées comme responsables par les Américains, la Direction générale des renseignements (GRU) et le Service fédéral de sécurité (FSB)[7]. Dans le même temps, un « hacker isolé » connu sous le pseudonyme de « Guccifer 2.0 » a revendiqué la responsabilité du piratage des réseaux et systèmes informatiques du DNC[8].

Ces opérations dans le cyberespace à l'encontre des réseaux et systèmes informatiques du DNC ont permis de dérober un grand nombre de données qui ont ensuite été rendues publiques en ligne sur WikiLeaks[9]. Ces fuites orchestrées des informations dérobées au DNC ont affecté le bon déroulement de la primaire démocrate et la campagne d'Hillary Clinton à l'élection présidentielle.

Le 20 avril 2018, le DNC a déposé plainte contre plusieurs acteurs, dont la Fédération de Russie, le GRU, Guccifer 2.0, WikiLeaks et son fondateur Julian Assange, ainsi que contre l'équipe de campagne de Donald Trump, concernant le piratage du DNC. Dans sa plainte, ainsi que dans la version amendée du 3 octobre 2018, le DNC relate sa compréhension des faits, le rôle de chaque acteur, la licéité des actes selon le droit américain et les dommages subis. Il est intéressant de noter que le 9 novembre 2018, la Cour a reçu une lettre du ministère de la Justice de la Fédération de Russie contenant une « Déclaration d'immunité de la Fédération de Russie[10] ». Dans cette déclaration, la Fédération de Russie rappelle son immunité souveraine en précisant qu'elle n'y renonce pas. Cette affaire, *Democratic National Committee v. the Russian Federation et al. (Case No 1 : 2018-cv-03501)*, est toujours pendante devant la cour du district sud de New York aux États-Unis.

Les opérations dans le cyberespace ne constituent qu'une partie des menaces numériques qui ont pesé sur l'élection présidentielle américaine de 2016. Deux autres menaces qui ont pesé sur cette élection doivent être mentionnées : les campagnes de manipulation de l'information et le rôle de l'entreprise britannique Cambridge Analytica.

L'élection présidentielle américaine de 2016 a donné lieu à des campagnes importantes de manipulation de l'information, principalement sur les réseaux sociaux. Le *Rapport d'enquête sur l'ingérence de la Russie dans les élections présidentielles de 2016* du procureur spécial Robert Muller décrit notamment les méthodes de l'entité russe Internet Research

Agency qui a mené des campagnes de manipulation de l'information sur les réseaux sociaux tout au long de la campagne électorale afin de favoriser Donald Trump et de dénigrer Hillary Clinton[11].

Le rôle de Cambridge Analytica est la dernière facette des menaces numériques contre l'élection américaine de 2016 que nous allons aborder dans ce chapitre. Cambridge Analytica est une société de communication stratégique combinant des outils d'exploration et d'analyse des données. Ainsi, ce type de société collecte des données sur les individus qu'elle cible, les analyse et fournit ensuite des outils de communication ciblés pour atteindre ces personnes et les influencer.

Plusieurs candidats à la primaire républicaine pour les élections présidentielles de 2016 ont bénéficié des services de la société Cambridge Analytica, notamment Ted Cruz, Ben Carson et Donald Trump. Elle a ensuite continué à fournir ses services à la campagne de Donald Trump jusqu'à son élection. Durant la campagne, cette société aurait moissonné les données de plus de cinquante millions d'utilisateurs de Facebook en vue de les exploiter pour favoriser le candidat républicain.

Bien que parfaitement légales, les activités de Cambridge Analytica se sont révélées particulièrement efficaces pour l'élection de Donald Trump. La facilité d'accès des données des utilisateurs de Facebook par Cambridge Analytica a entraîné de très sévères critiques à l'encontre du réseau social et plus largement du modèle de monétisation et de protection des données aux États-Unis. Cambridge Analytica a cessé ses activités en 2018. Cependant, ce n'est pas un cas isolé et de nombreuses sociétés offrent des services similaires.

Les élections françaises de 2017 : une meilleure anticipation

Le 7 mai 2017, Emmanuel Macron était élu président de la République française. Six mois plus tôt, les élections présidentielles françaises de 2017 avaient été marquées par des incidents de cybersécurité et des campagnes de désinformation, principalement à l'encontre du candidat Emmanuel Macron et de son parti En Marche !

La cybersécurité a été une préoccupation importante du gouvernement français lors de l'élection de 2017, notamment en raison du précédent américain. En février 2017, le président François Hollande a demandé au Conseil de défense et de sécurité nationale (CDSN) de préparer des mesures spécifiques sur le risque d'intervention, y compris les menaces liées à la cybersécurité, en vue des élections[12]. Le 15 février, Jean-Marc Ayrault, alors ministre des Affaires étrangères, s'adressait au Parlement et déclarait que la France n'accepterait aucune ingérence dans son processus électoral, que ce soit de la part de la Russie ou d'autres pays[13].

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a lancé plusieurs alertes sur les risques numériques à l'encontre des élections, qui ont notamment conduit à la suppression de la possibilité pour les Français établis à l'étranger de voter en ligne lors des élections législatives de juin 2017[14]. L'ANSSI et la Commission nationale de contrôle de la campagne électorale en vue de l'élection présidentielle (CNCCEP) ont rappelé que l'ANSSI était chargée de la cybersécurité des élections, mais que les partis et les candidats étaient responsables de leur propre cybersécurité.

Le 3 mai 2017, le mercredi précédant le second tour de l'élection présidentielle, les deux candidats au second tour, Marine Le Pen et Emmanuel Macron, s'affrontaient lors du traditionnel débat télévisé. Durant le débat, Marine Le Pen a lancé à l'encontre de son adversaire : « [J]'espère qu'on n'apprendra pas que vous avez un compte offshore aux Bahamas[15]. » Cette rumeur, généralement appelée « MacronGate », semble être née deux heures avant le début du débat, lorsque deux documents, apparus sur le

forum 4chan, ont été largement diffusés sur les réseaux sociaux, suggérant qu'Emmanuel Macron avait créé une société à des fins d'évasion fiscale.

Le vendredi 5 mai, dans la soirée, des giga-octets de courriels et de documents dérobés à En Marche ! étaient publiés en ligne. Cette fuite de documents a été désignée par l'expression « Macron Leaks[16] ». Ces documents ont d'abord été publiés sur *Pastebin* sous le titre EMLEAKS et postés sur le forum 4chan[17], avant d'être largement partagés sur les réseaux sociaux[18]. Le 31 juillet, WikiLeaks a republié de nombreux documents issus de ces fuites sous le titre de « Macron Campaign Emails[19] ».

Le service du renseignement militaire russe, le GRU, est généralement considéré comme responsable de la campagne d'hameçonnage et d'autres opérations dans le cyberespace pendant les élections présidentielles françaises de 2017[20]. Il faut cependant noter que le 1er juin 2017, le directeur de l'ANSSI Guillaume Poupard a déclaré que ce piratage « était si simple et générique qu'il a pu être commis par quasiment n'importe qui. Les responsables peuvent être dans n'importe quel pays […]. On peut imaginer qu'une personne seule est responsable[21] ». Il est intéressant de noter que le 9 mai 2017 l'amiral Michael S. Rogers, alors chef de l'Agence de sécurité nationale (NSA) et du Commandement Cyber américain (USCYBERCOM), a déclaré lors d'une audition publique devant la Commission sénatoriale américaine des services armés, qu'ils avaient connaissance des activités russes et qu'ils avaient mis en garde leurs homologues français[22]. Cette déclaration suggère qu'il considère la Fédération de Russie comme étant responsable de ces opérations dans le cyberespace au cours de l'élection française. Le gouvernement français, que ce soit avant ou après l'élection d'Emmanuel Macron, n'a jamais officiellement attribué ces cyberopérations, et plus largement les tentatives d'ingérence pendant la campagne électorale, à un quelconque pays étranger.

Les opérations cyber contre les processus électoraux

Dans le cadre d'un processus électoral, de nombreuses cibles différentes peuvent être visées par des opérations dans le cyberespace dans le but d'agir sur le processus électoral en cours. Deux catégories de cibles principales sont à distinguer : les candidats et les partis ; le processus électoral lui-même. Enfin, d'autres cibles moins directes, comme des médias par exemple, peuvent aussi faire l'objet d'opérations dans le cyberespace.

Il convient de s'interroger sur les motivations des acteurs utilisant les TIC à l'encontre des processus électoraux et sur les conséquences de leurs actes. Dans une interview auprès de *mediametrics.ru* sur les guerres de l'information et leur rôle dans l'élection de Donald Trump, Konstantin Rykov, un ex-membre du Parlement russe, déclarait : « On a réussi, [Donald] Trump est président. Malheureusement, Marine [Le Pen] n'est pas devenue présidente. Une chose a fonctionné, mais pas l'autre[23]. » Influencer les résultats d'une élection pour faire élire un candidat particulier peut sembler être l'objectif principal des campagnes de manipulation de l'information et des opérations dans le cyberespace en période électorale. Cet objectif semble néanmoins difficile à atteindre. De notre point de vue, l'objectif des opérations dans le cyberespace à l'encontre de l'infrastructure électorale et plus généralement des différents partis en lice est à chercher ailleurs.

Il paraît improbable de réussir à modifier le résultat d'un scrutin dans un sens donné, c'est-à-dire de faire élire un candidat en particulier, seulement par le biais d'opérations dans le cyberespace. Même dans les cas où le scrutin serait intégralement fait par le biais de machines à voter électroniques, ces machines ne sont généralement pas connectées à Internet ni interconnectées entre elles. Pouvoir modifier massivement le scrutin dans

un sens donné demanderait donc de pirater à l'avance chaque machine afin d'en affecter le fonctionnement et donc de modifier la manière dont elles enregistreront les votes. Une telle action demanderait un déploiement important de moyens humains pour accéder à chaque machine. Dans le cas d'un vote se déroulant sur Internet, il serait probablement plus facile de modifier le résultat. Néanmoins, qu'il s'agisse d'un vote par voie électronique ou par le biais de machines à voter électroniques, il faudrait réussir à procéder à ces manipulations sans éveiller de soupçons de façon à éviter l'invalidation partielle ou totale de l'élection. Toutes ces conditions limitent fortement la probabilité de modifier le résultat dans un sens donné par le biais d'opérations dans le cyberespace visant l'infrastructure électorale.

Ce type d'opérations dans le cyberespace, qui peuvent être couplées avec d'autres formes d'opérations, par exemple des manipulations d'information ou des campagnes d'information ciblées, peut néanmoins avoir des conséquences importantes à court et à long terme sur le fonctionnement des démocraties. Elles peuvent notamment entraîner l'invalidation du scrutin ou du résultat de certains bureaux de vote, où les machines à voter ou les listes d'émargement auront été compromises, engendrant alors un déséquilibre dans la prise en compte des résultats du scrutin. Plus généralement, le fait que des irrégularités puissent être constatées pendant le scrutin pourrait aussi servir les intérêts des candidats perdants de l'élection. En effet, ces éléments pourraient être utilisés pour contester la validité du scrutin. Ainsi, une puissance étrangère ou un groupe souhaitant apporter son soutien à un candidat minoritaire seraient fondés à agir en ce sens pour lui permettre par la suite de contester l'élection et de montrer le caractère non équitable du scrutin.

À plus long terme, ces actions et leurs conséquences pourraient servir d'amplificateur à la crise démocratique que traversent la plupart des démocraties. Celle-ci se caractérise par la diminution du taux de

participation aux différents scrutins, mais aussi par la contestation croissante des résultats et de la légitimité des processus électoraux. Des incidents causés par des opérations dans le cyberspace à l'encontre de certaines composantes de l'infrastructure électorale instilleraient le doute dans l'esprit des électeurs quant à la validité et la régularité des scrutins. Ainsi, ils viendraient alimenter la diminution de la confiance des électeurs dans les processus électoraux, causant à terme un risque pour la viabilité de ces processus.

Les atteintes à la liberté de choix des électeurs

Le développement des TIC offre de nouveaux vecteurs pour influencer la liberté de choix des électeurs comme le soulignent les élections présidentielles américaine et française. L'exemple américain est particulièrement intéressant car il montre la diversité de ces menaces. Le premier type de menaces recouvre les manipulations de l'information. Depuis quelques années la propagation d'informations fausses, travesties ou sorties de leur contexte est un sujet de préoccupation pour la plupart des gouvernements.

Le développement des TIC et des réseaux sociaux a permis l'émergence de nouveaux modes de communication, moins centralisés et plus directs, permettant aux informations de circuler directement entre individus et hors du contrôle des gouvernements ou des médias traditionnels. Cette révolution des modes de communication et d'accès à l'information représente une chance pour la revitalisation de nos démocraties. Néanmoins, elle a aussi démultiplié la circulation d'informations fausses ou manipulées. Cette situation est favorisée par le contexte général de défiance à l'égard des sources traditionnelles d'information qui s'est installé dans de nombreux États. Il est important de noter que ces manipulations de

l’information prennent des formes très diverses, avec des niveaux de sophistication et d’intensité différents. De la même manière, les acteurs responsables de ces campagnes de manipulation de l’information ont des profils et des motivations divers.

Le second type de menace est plus insidieux et recouvre les techniques de ciblage informationnel des électeurs. Les TIC permettent, en effet, de mieux identifier chaque électeur individuellement et d’adapter les informations qu’il reçoit en fonction de ses centres d’intérêt et de ses orientations politiques. C’est l’exemple des activités de la société Cambridge Analytica durant les élections américaines ou encore de la société canadienne AggregateIQ pendant la campagne du Brexit en Grande-Bretagne[24].

Pendant des années, divers acteurs ont récolté des données personnelles sur différents réseaux sociaux, notamment par le biais d’applications disponibles sur ces réseaux. Facebook, et en particulier sa plateforme Open Graph lancée en 2010, ont ainsi permis aux développeurs d’applications pour ce réseau social de collecter de nombreuses données sur les utilisateurs de ces applications et leurs contacts sur Facebook. À titre d’exemple, l’application « Thisisyourdigitallife » lancée en 2013 par Aleksandr Kogan et la société Global Science Research invitait ses utilisateurs à remplir un test de personnalité. Pendant ses deux années d’existence, cette application a collecté des informations personnelles sur les 270 000 personnes ayant choisi de remplir le test de personnalité qu’elle proposait. En remplissant ce test, les utilisateurs autorisaient aussi l’application à prendre connaissance des mentions « j’aime » qu’ils avaient attribuées sur Facebook et plus généralement de leur activité sur le réseau social. En outre, les conditions d’utilisation de Facebook et de sa plateforme Open Graph autorisaient ce type d’application à collecter des informations sur leurs utilisateurs mais aussi sur leurs contacts sur ces réseaux. Ainsi, avec seulement 270 000 utilisateurs l’application « Thisisyourdigitallife » aurait été en mesure de

collecter des données personnelles sur 30 à 50 millions de personnes selon les estimations. En 2015, Facebook a modifié les conditions d'utilisation d'Open Graph limitant notamment les possibilités d'accès aux contacts des utilisateurs de ces applications. Néanmoins, grâce à l'importante masse de données collectées par ces applications, des algorithmes de profilage des utilisateurs des réseaux sociaux ont permis de développer des mécanismes de communication ciblés à des fins commerciales mais aussi à des fins politiques. Ainsi, les données collectées par l'application « Thisisyourdigitallife » sont devenues la propriété de la société SCL Group, qui les a notamment utilisées pour le développement des activités d'une de ses filiales, Cambridge Analytica[25].

Les révélations publiques sur l'influence de Cambridge Analytica sur l'élection de Donald Trump et la facilité avec laquelle cette société a pu accéder aux données de nombreux utilisateurs de Facebook ont provoqué un scandale important aux États-Unis. Le directeur de Facebook, Mark Zuckerberg, a ainsi été auditionné par plusieurs commissions parlementaires américaines pour s'expliquer sur le traitement des données personnelles par Facebook. Cette situation a ravivé le débat sur la protection des données personnelles outre-Atlantique et sur la monétisation de ces données qui est aujourd'hui le modèle économique sur lequel se fonde la puissance des GAFAM. En effet, à l'inverse de l'Union européenne et des États européens qui disposent de cadres législatifs assez restrictifs et contraignants sur l'utilisation des données personnelles, les États-Unis offrent un cadre beaucoup plus permissif favorisant ce type de pratiques.

Le 30 décembre 2019, Andrew Bosworth, un des cadres dirigeants de Facebook, a publié sur le réseau interne de Facebook un texte rendu public par le *New York Times*[26] et qu'il a ensuite publié publiquement à son tour sur Facebook[27]. Il affirme que Facebook a joué un rôle important dans l'élection de Donald Trump. Ainsi, dans ce long texte, il minimise le rôle

des campagnes russes de manipulation de l'information et de Cambridge Analytica, avant de souligner que :

> Alors, est-ce que Facebook est responsable de l'élection de Donald Trump ? Je pense que la réponse est oui, mais pas pour les raisons que l'on croit. Il n'a pas été élu à cause de la Russie, de la désinformation ou de Cambridge Analytica. Il a été élu parce qu'il a mené la meilleure campagne de publicité numérique que j'aie jamais vue de la part d'un annonceur. Point final.

Il poursuit en précisant comment les outils de publicité numérique proposés par Facebook ont été mis à profit par l'équipe de campagne de Donald Trump. Il questionne ensuite la politique publicitaire de Facebook, soulignant qu'à titre personnel il aurait souhaité pouvoir tout mettre en œuvre pour empêcher l'élection de Donald Trump. Toutefois, il ne lui semble pas souhaitable et il serait même dangereux à ses yeux de vouloir réguler le recours aux outils publicitaires dans les campagnes électorales, comparant ainsi l'adoption de la politique publicitaire restrictive à l'anneau dans *Le Seigneur des anneaux* :

> Je pense au *Seigneur des anneaux* en ce moment. Plus précisément lorsque Frodon offre l'anneau à Galadrial et qu'elle imagine utiliser le pouvoir à bon escient, dans un premier temps, mais sait que cela finira par la corrompre. Aussi tentant qu'il soit d'utiliser les outils à notre disposition pour changer le résultat, je suis persuadé que nous ne devons jamais faire cela ou nous deviendrons ce que nous craignons.

Cette publication d'Andrew Bosworth expose différents outils numériques pouvant servir à influencer le choix des électeurs, qu'il s'agisse

de manipulations de l'information, de communication stratégique ou de publicité sur les réseaux sociaux. Il montre les liens entre eux, tant dans leur conduite que dans leurs conséquences. Cela nous amène à nous interroger sur les moyens qui peuvent être mis en œuvre pour endiguer ces menaces.

La panoplie des réponses possibles

Face aux menaces numériques en période électorale, chaque État s'efforce de mettre en place les meilleures solutions pour protéger le scrutin et assurer la liberté de choix des électeurs[28]. Ces efforts visent généralement à contrer les opérations dans le cyberespace et les campagnes de manipulation de l'information, ainsi qu'à identifier à l'avance les auteurs potentiels de ces actions.

Il est intéressant de noter que, dans la perspective des élections présidentielles américaines de 2020, l'US Cyber Command a lancé des opérations pour dissuader et perturber les acteurs russes qui ont été identifiés comme interférant dans de précédentes élections aux États-Unis – principalement ceux impliqués dans des campagnes de manipulation de l'information[29].

Après les différentes campagnes de manipulation de l'information lors du scrutin présidentiel de 2017, la France s'est dotée d'un nouveau cadre législatif pour lutter contre les manipulations de l'information en 2018[30]. Cette loi vise spécifiquement à lutter contre les manipulations de l'information en période électorale. Le secteur privé se montre aussi actif sur ces questions. La société multinationale Microsoft avait, par exemple, mis en garde contre le risque élevé de tentatives d'ingérence par des moyens numériques lors des élections européennes de 2019 et a proposé des solutions commerciales à différents États européens[31]. Cette initiative fait partie du programme de Microsoft intitulé *Defending Democracy Program*

qui vise à protéger les processus électoraux contre les opérations dans le cyberespace et les campagnes de manipulation de l'information.

Il existe une perméabilité entre les différentes formes de menaces numériques en période électorale. Ainsi, il peut y avoir des interconnexions entre les opérations dans le cyberespace, les campagnes de manipulation de l'information et les campagnes de communication stratégique, tant dans leur conduite que dans leurs effets : dans leur conduite lorsque, par exemple, des opérations dans le cyberespace à l'encontre de partis politiques sont utilisées pour dérober des données qui serviront ensuite dans des campagnes de manipulation de la liberté de choix des électeurs ; dans leurs effets en montrant que ce n'est pas un type de menaces numériques donné qui s'est montré décisif, mais plutôt l'accumulation des différentes actions.

*

L'analyse croisée des campagnes de manipulation de l'information et des pratiques de communication stratégique incite à s'interroger : le problème réside-t-il réellement dans ces pratiques ou sont-elles des symptômes d'un problème plus large ? De notre point de vue, ces pratiques s'inscrivent dans le problème plus large de l'accès à l'information. En effet, la révolution des TIC a permis de diversifier et de renouveler la manière dont les individus ont accès à l'information, offrant notamment de nouveaux moyens de communication décentralisés et plus directs.

Face à cette révolution, le citoyen se retrouve bien souvent seul pour faire le tri dans le flux exponentiel d'informations qu'il reçoit. Ainsi, de notre point de vue, les actions contre les campagnes de manipulation de l'information constituent des palliatifs nécessaires, mais il faut aussi s'attaquer au cœur du problème : l'éducation des citoyens dans l'accès à l'information et la hiérarchisation des sources.

Il existe de nombreuses initiatives en ce sens aujourd'hui qui méritent d'être saluées. Une telle action est aussi le meilleur moyen de lutter efficacement contre un autre problème lié aux TIC : la vitesse du développement et des évolutions technologiques. En cherchant à lutter contre les moyens mis en œuvre, les États se retrouvent souvent en retard par rapport à l'évolution des technologies et des techniques. Ce n'est qu'en s'attaquant au cœur du problème, la manière dont ses technologies sont appréhendées et utilisées par les citoyens, que l'on pourra avoir une action significative et assurer la résilience des sociétés démocratiques.

Pour aller plus loin

DELERUE François, *Cyber Operations and International Law*, Cambridge, Cambridge University Press, 2020, chap. 5.

JEANGÈNE VILMER Jean-Baptiste, ESCORCIA Alexandre, GUILLAUME Marine, HERRERA Janaina, *Les Manipulations de l'information*, rapport conjoint du CAPS (Centre d'analyse, de prévision et de stratégie du ministère de l'Europe et des Affaires étrangères) et de l'IRSEM (Institut de recherche stratégique de l'École militaire du ministère des Armées), 2018.

HOLLIS Duncan B., « Russia and the DNC Hack : What future for a duty of non-intervention ? – Opinio Juris », *Opinio Juris*, 27 juillet 2016 (en ligne).

OHLIN Jens David, « Did Russian cyber interference in the 2016 election violate international law ? », *Texas Law Review*, 2016, n° 95.

« The Cambridge Analytica Files », *The Guardian*, 2018. Voir https://www.theguardian.com/news/series/cambridge-analytica-files.

CHAPITRE 16

Panorama des mesures prises contre les manipulations de l'information

Jean-Baptiste Jeangène Vilmer

À l'exception de quelques États d'Europe centrale, nordique et orientale pour lesquels les attaques informationnelles venant de l'Est n'ont pas vraiment cessé avec la fin de la guerre froide, tous ceux qui, à l'« Ouest », avaient mis en place des mesures défensives contre les opérations soviétiques ont « désarmé » dans les années 1990 et se sont donc trouvés dépourvus lorsque, vingt ans plus tard, le besoin s'est fait sentir de se défendre à nouveau contre des attaques informationnelles étatiques de grande ampleur[1]. La prise de conscience a été graduelle – et elle continue de croître partout dans le monde – mais semble s'être accélérée dans les années 2010, en trois étapes.

La première est l'annexion de la Crimée en 2014 et la guerre du Donbass : l'offensive russe en Ukraine est devenue depuis un cas d'école de guerre dite « hybride[2] », dont la « guerre informationnelle » est une partie, et elle a été le premier accélérateur de la prise de conscience des vulnérabilités étatiques. Cependant, l'Ukraine étant aussi un cas particulier, compte tenu de son histoire avec la Russie et du fait que les populations

visées étaient majoritairement russophones, ce risque a surtout trouvé un écho dans les pays présentant l'une ou l'autre de ces spécificités, notamment les États baltes. L'Ukraine, directement visée, prenait elle-même plusieurs mesures, dont certaines assez drastiques comme l'interdiction des médias russes. Mais, sous la pression d'un certain nombre d'États plus préoccupés que les autres, cette prise de conscience s'est généralisée à l'Organisation du traité de l'Atlantique nord (OTAN) et l'Union européenne (UE).

La deuxième étape qui a internationalisé la perception de la menace est l'ingérence russe dans la campagne présidentielle américaine de 2016. Autant les actions précédentes pouvaient convaincre certains grands États d'Europe occidentale ou d'Amérique du Nord qu'ils étaient en quelque sorte « hors d'atteinte » à la fois des capacités et des ambitions russes en la matière, autant le cas américain a démontré à la face du monde que personne, pas même la première puissance mondiale, n'était à l'abri. Cette affaire a eu l'effet immédiat de mettre en alerte tous les autres États. Une autre ingérence électorale dans une grande puissance l'année suivante, la France, avec l'opération dite des « Macron Leaks », a confirmé cette vulnérabilité partagée et donc la nécessité de mieux se protéger. L'accumulation des mesures – organisationnelles, législatives ou éducationnelles – prises par les États est exponentielle à partir de 2017.

La troisième étape dans cette prise de conscience en escalier a consisté à globaliser la perception de la menace, qui n'est ni seulement russe, ni seulement étatique. Cela s'est notamment traduit par un « pivot asiatique » plaçant la Chine au centre des préoccupations – ce qui a toujours été le cas pour quelques pays, dont Taïwan, l'Australie et Singapour notamment, la nouveauté étant que la question de l'influence chinoise et, plus précisément, de ses manœuvres informationnelles, est désormais posée avec autant d'inquiétude à Washington, Bruxelles ou Addis-Abeba. Il en va de même pour les acteurs non étatiques : la prise de conscience avait déjà eu lieu

depuis le début des années 2000 concernant le cas particulier des groupes armés djihadistes, d'abord al-Qaida puis Daech (et avait amorcé des tentatives de réponses coordonnées), mais elle s'étend désormais aux mouvements populistes, nationalistes et aux extrêmes de toute sorte, ainsi qu'aux entreprises qui font de la désinformation un business. En d'autres termes, il est clair désormais que la menace est globale, protéiforme et multiscalaire. Rares sont ceux qui ne s'estiment pas concernés. Des îles Féroé aux îles Fidji en passant par le Mali, les Philippines et le Brésil, la prise de conscience est quasi universelle, à des degrés divers bien sûr, certains s'estimant (à tort ou à raison) plus ou moins menacés que d'autres.

Dans ce contexte, la question que pose ce chapitre est celle de savoir quelles sont les réponses : quelles mesures les États et les sociétés civiles ont-ils prises pour se défendre contre les manipulations de l'information ? Ce que l'on peut appeler la « défense informationnelle » (*information defense*)[3] est autant la défense *de* que la défense *par* l'information. On distinguera les mesures prises par les États, la coopération internationale et la société civile, avant d'en pointer les limites[4].

La mobilisation des États

Face aux manipulations de l'information dont les conséquences, pendant les élections ou en dehors, sont désormais prises au sérieux, les États ont pris depuis le milieu des années 2010 un certain nombre de mesures allant du design organisationnel, c'est-à-dire de la manière la plus optimale d'organiser l'administration[5], à la régulation des médias, en passant par le rôle des parlements, qui enquêtent et légifèrent, et la sensibilisation du public.

Le design organisationnel

Le premier réflexe des États – en tout cas des démocraties libérales – a été de modifier leur organisation interne. Ils l'ont fait différemment, car les cultures stratégiques et administratives ne sont pas les mêmes. Tous ont fait le constat que face à une menace « hybride » en ce qu'elle mêle et parfois confond le civil et le militaire, l'étatique et le non-étatique, et plusieurs domaines (non seulement la défense et la diplomatie mais aussi la culture, la justice, etc.), la priorité était d'adopter une approche globale et donc de transversaliser, décloisonner des services qui travaillent généralement en silos. *A minima*, il s'agit donc de connecter des compétences éparpillées, en créant des « comités » ou des « réseaux », comme le Réseau sur l'influence informationnelle finlandais, créé dès 2014 et regroupant une trentaine d'experts gouvernementaux pour identifier, analyser et répondre aux tentatives hostiles d'ingérence étrangère. La plupart des pays européens ont aujourd'hui un dispositif similaire. Il peut s'agir d'un groupe de travail temporaire ou d'un comité permanent : dans tous les cas, il ne fait que réunir des personnes déjà en poste. Certains vont plus loin en allouant un budget spécifique et en créant des postes pour constituer une structure dédiée à plein temps à la lutte contre les manipulations de l'information, soit au sein d'un service existant, soit en la créant *ex nihilo*.

Qu'il s'agisse d'une mise en réseau de l'existant ou de la création d'une nouvelle structure, se pose la question épineuse du rattachement institutionnel, qui se règle relativement facilement dans les États ayant déjà une culture transversale et horizontale, notamment les États scandinaves, ou les petits États, comme les pays Baltes, dans lesquels les équipes, plus réduites, ont davantage de chance de se connaître et de travailler ensemble. En général, le réseau ou la structure est piloté par les services du Premier ministre, une agence interministérielle ou encore un ministère donné (la Justice au Danemark et aux Pays-Bas, la Culture en Lettonie, le ministère des Communications et de l'Information à Singapour, etc.). Le ministère

des Affaires étrangères britannique (FCO) accueille une cellule interministérielle d'une vingtaine de personnes ; le ministère de l'Intérieur en République tchèque héberge un centre de lutte contre le terrorisme et les menaces hybrides (CTHT) d'une vingtaine de personnes également ; et le ministère de l'Intérieur (Home Affairs) en Australie accueille l'équipe du coordinateur national en charge de la contre-ingérence.

Ces exemples témoignent d'ailleurs de la grande variété de focales retenues : les manipulations de l'information au sens strict, l'influence et/ou l'ingérence (une difficulté étant de savoir où finit l'une et où commence l'autre), ou encore les menaces « hybrides », qui sont même parfois, comme en République tchèque, associées aux menaces terroristes[6].

Le cas américain est particulier en ce qu'il n'y a pas *une* mais *des* structures dédiées (le Global Engagement Center créé en 2016 au sein du département d'État, mais aussi de nombreuses *task forces* dédiées à la lutte contre la désinformation et/ou l'influence étrangère, dans d'autres administrations, dont le département de la Justice et le département de la Sécurité intérieure). Leur problème est donc moins un manque de ressources qu'un manque de coordination car, sur ce sujet hautement politique, aucune direction claire ne vient du Conseil de sécurité nationale et de la Maison Blanche.

Parmi les États qui ont mis en réseau leurs compétences existantes sans pour autant créer des structures dédiées permanentes et, donc, des postes supplémentaires, certains sont paralysés par des considérations bureaucratiques et budgétaires mais pour d'autres, comme Singapour, c'est un choix assumé, pour montrer que la lutte contre les manipulations de l'information est « l'affaire de tous » et ne pas risquer que la concentration des moyens dans une structure unique fasse que les autres services ne se sentent plus concernés[7].

Le rôle des parlements

Les parlements contribuent à la lutte contre les manipulations de l'information en enquêtant et en légiférant. Les principales enquêtes, aux États-Unis, au Royaume-Uni et en Australie, étant publiques et très suivies par les médias, elles permettent aussi d'informer et sensibiliser la population et, en exposant les responsables présumés, d'avoir peut-être un effet dissuasif. Elles sont le fait des services de police judiciaire (aux États-Unis, le FBI a commencé à enquêter sur « l'affaire russe » en juillet 2016) et des parlements, qui produisent en général des rapports très détaillés et très utiles, comme celui des sénateurs démocrates américains de janvier 2018[8] ou du comité pour le numérique, la culture, les médias et le sport de la Chambre des communes britannique en février 2019[9]. En décembre 2019, le parlement australien a à son tour établi un Comité restreint sur l'ingérence étrangère par les médias sociaux qui devrait remettre un rapport d'ici 2022[10]. Il est à noter que les rapports parlementaires ne s'inscrivent pas nécessairement dans une enquête visant un cas d'ingérence suspecté ou avéré. À Singapour, c'est pour préparer sa loi contre la désinformation que le parlement a créé en janvier 2018 un Comité restreint sur les mensonges délibérés en ligne qui, après de nombreuses auditions, y compris d'experts étrangers, a rendu son rapport en septembre 2019[11]. Au Royaume-Uni, le comité susnommé de la Chambre des communes a également publié un rapport sur *Misinformation in the COVID-19 Infodemic* en juillet 2020.

D'autre part, les parlements légifèrent. Certains États disposaient déjà, depuis parfois très longtemps, d'une législation dans ce domaine. En France par exemple, la loi sur la liberté de la presse de 1881 punissait déjà « la publication, la diffusion ou la reproduction, par quelque moyen que ce soit, de nouvelles fausses, de pièces fabriquées, falsifiées ou mensongèrement attribuées à des tiers lorsque, faite de mauvaise foi, elle aura troublé la paix publique, ou aura été susceptible de la troubler ». Mais ces anciennes dispositions étaient parfois incomplètes, ou inadaptées à l'ère numérique

dans laquelle nous vivons désormais et qui a changé non pas la nature des manipulations de l'information (qui ont toujours existé) mais les moyens et la vitesse de leur propagation, puisqu'il est désormais possible de toucher des millions de personnes en quelques minutes. Il est donc apparu nécessaire soit de mettre à jour, soit dans d'autres cas de créer de toutes pièces, une législation adaptée.

Certaines démocraties libérales se sont engagées dans cette voie. L'Allemagne la première avec sa fameuse loi « Netzwerkdurchsetzungsgesetz » (NetzDG), entrée en vigueur au 1er janvier 2018, forçant les plateformes numériques à supprimer les messages « de toute évidence illégaux » dans les 24 heures, au risque d'encourir une amende susceptible d'aller jusqu'à 50 millions d'euros. En France, une loi contre la manipulation de l'information a été adoptée par l'Assemblée nationale en novembre 2018 puis validée par le Conseil constitutionnel le mois suivant. En Israël, un jugement de la Cour suprême interdit, à compter de mars 2019, les publicités anonymes et contraint les faux comptes utilisés pour faire de la propagande et les bots à s'identifier. Taïwan est un autre exemple, avec la loi « anti-infiltration » de décembre 2019 qui contient certaines mesures pour lutter contre la désinformation.

Le fait est cependant que la plupart des législations ont été adoptées dans des pays qui ne peuvent pas être considérés comme des démocraties libérales. La Chine et la Russie passent régulièrement des lois criminalisant le fait de diffuser des rumeurs susceptibles de nuire à l'ordre social. Lorsque la Malaisie (avril 2018), le Cambodge et le Kenya (mai 2018), la Biélorussie (juin 2018), l'Égypte (juillet 2018), l'Algérie (avril 2020), le Kirghizistan (juin 2020) ou encore le Brésil (juillet 2020) ont également adopté des législations dans ce domaine, ils ont été vivement critiqués par les organisations de défense des droits humains. Dans ces contextes où la liberté de la presse est déjà menacée, voire inexistante, ces mesures

législatives ne font que la dégrader davantage et renforcer le contrôle de l'exécutif sur sa population. Le cas singapourien est également ambivalent : la loi sur la protection contre les mensonges en ligne et la désinformation (POFMA), adoptée par le parlement en mai 2019, a été vivement critiquée dans certains médias occidentaux[12] pour avoir été utilisée contre un parti d'opposition – une affaire qui suscite un débat à Singapour même, où elle a été portée devant la Haute Cour de justice.

La sensibilisation de la population

Les démocraties libérales ont vite compris que les mesures précédentes ne suffiraient pas si la population dans son ensemble n'était pas consciente des dangers des manipulations de l'information. Pour la sensibiliser, les États – certains plus que d'autres naturellement – ont donc mis en place un éventail de mesures parmi lesquelles la formation des fonctionnaires[13] et des partis politiques en période électorale[14], mais aussi la mise en ligne de sites Internet dédiés pour informer le grand public[15] ou la distribution de brochures[16].

Une autre mesure préventive est bien entendu l'ajout ou le développement de l'éducation aux médias dans les programmes scolaires[17]. Le financement de la société civile est également important[18], comme le soutien à la recherche, qui implique de financer et parfois co-publier des études, comme l'a fait le MSB avec l'université de Lund pour leur *Handbook* sur les opérations d'influence.

La régulation des médias

Parmi les mesures prises par les États, certaines visent spécifiquement les médias qui, avec les plateformes numériques, sont les principaux vecteurs des manipulations de l'information. Ces mesures consistent

généralement à renforcer le pouvoir des autorités de régulation des médias comme l'Ofcom britannique ou le Conseil supérieur de l'audiovisuel français ; et contraindre les médias à faire preuve de transparence quant à leurs relations financières avec un État étranger, comme le fait le *Foreign Agent Registration Act* aux États-Unis. À la demande du département de la Justice, RT et Sputnik se sont ainsi enregistrés comme « agents de l'étranger ». La Russie a adopté une loi similaire, dans un contexte où la liberté de la presse est bien moindre que dans les démocraties occidentales[19], de sorte que, dans les faits, ce statut d'agent de l'étranger peut être utilisé pour pousser un certain nombre de médias à la fermeture. Enfin, certains États ont choisi d'interdire purement et simplement certains médias, comme l'Ukraine l'a fait avec les médias russes (73 chaînes de télévision interdites entre 2014 et 2016) et plusieurs sites russes en mai 2017 (VKontakte, Odnoklassniki, Yandex, Mail.ru). De même, l'Indonésie a également choisi de bloquer des sites ou des réseaux sociaux pour lutter contre les manipulations de l'information – un choix généralement critiqué par les démocraties libérales et les organisations de défense des droits humains.

La coopération internationale

Les menaces que posent les manipulations de l'information étant par nature transnationales, non seulement parce qu'une attaque peut venir de l'étranger mais aussi et surtout parce qu'Internet n'a pas de frontière, elles posent à la société internationale un défi global qui nécessite des réponses coordonnées. La coopération internationale est donc cruciale. Elle n'a cessé de progresser, en particulier depuis 2014. On peut distinguer plusieurs couches : le partage du renseignement, principalement bilatéral, les formats multilatéraux (UE, OTAN, G7) et le rôle des think tanks.

Le partage du renseignement

La première couche, qui a toujours existé, est le partage du renseignement – qui reste toutefois limité car, dans ce domaine comme dans celui du cyber, partager des informations revient aussi à partager des vulnérabilités ; les États sont donc souvent réticents. À quelques exceptions près dont les Five Eyes[20], ce type de coopération est généralement bilatéral, entre deux États qui se font confiance. Il est difficile de s'ouvrir à un plus grand nombre, et le niveau de l'information partagée (ce qu'on dit) dépend du niveau de confiance du partenaire (à qui on le dit). Il y a par exemple une réticence à trop partager avec des services qu'on estime trop pénétrés par l'adversaire, ou des États dont le leadership politique est considéré comme trop ambivalent à l'égard de cet adversaire.

Néanmoins, entre alliés de longue date, comme la France et les États-Unis par exemple, le partage de renseignement fonctionne bien et c'est d'ailleurs l'une des leçons que l'on peut tirer de la bonne gestion de l'opération dite des « Macron Leaks » en 2017. Si la France a appris des États-Unis, c'est autant en tirant les leçons des erreurs commises par l'administration Obama durant la campagne présidentielle de 2016, qu'en bénéficiant du renseignement américain. À plusieurs reprises durant la campagne française, les services américains ont alerté les services français sur les « activités russes[21] ».

Les formats multilatéraux : UE, OTAN, G7

La deuxième couche est celle des formats multilatéraux, dont les plus actifs dans la lutte contre les manipulations de l'information sont l'UE, l'OTAN et le Groupe des sept (G7).

Premièrement, pour répondre aux conclusions du Conseil européen des 19-20 mars 2015 qui soulignaient « la nécessité de contrer les campagnes

de désinformation menées par la Russie » et qui invitaient la haute représentante à élaborer un plan d'action sur la communication stratégique, la division Communication stratégique du Service européen pour l'action extérieure (SEAE) a créé trois équipes : une « *task force* de communication stratégique orientée vers le voisinage oriental » (East StratCom Task Force), active depuis septembre 2015, composée d'une quinzaine de personnes, qui diffuse son travail sur son site Internet « EU vs Disinformation » (euvsdisinfo.eu), dans une *Disinformation Review* hebdomadaire et sur les réseaux sociaux sous le nom de « briseurs de mythes » (*EU Mythbusters*) ; une *task force* « Sud », créée en 2015 et composée de quatre personnes, qui lutte contre le discours djihadiste ; et une *task force* « Balkans occidentaux » créée en 2017, composée de trois agents, qui se concentre sur la défense de l'image de l'UE dans la région.

En 2016, la Commission européenne a adopté un cadre commun en matière de lutte contre les menaces hybrides[22]. À la suite d'une résolution du parlement européen de juin 2017 qui lui demande d'étudier l'éventualité « d'une intervention législative afin de limiter la publication et la diffusion de faux contenus[23] », la Commission européenne se saisit du sujet. La Commissaire pour l'économie et la société numériques constitue un groupe d'experts qui rend un rapport en mars 2018 faisant un certain nombre de recommandations. Complété par une consultation publique, il sert de base à la communication sur la lutte contre la désinformation que la Commission publie le mois suivant. Celle-ci propose l'élaboration d'un « code de bonnes pratiques contre la désinformation », qui est publié en juillet 2018. En octobre, le code est signé par Facebook, Twitter, Google, Mozilla et plusieurs associations professionnelles, s'engageant à faire des progrès pour lutter contre la désinformation en ligne, notamment en supprimant davantage de faux comptes et en limitant la visibilité des sites favorisant la désinformation. En mai 2019, Microsoft signe à son tour. En octobre de la même année, les signataires publient les premiers rapports d'autoévaluation

sur la mise en œuvre de leurs engagements. Cette procédure a la vertu de pousser les plateformes à davantage de transparence quant aux mesures prises, à la fois quantitativement et qualitativement, et met en évidence un réel effort de leur part mais aussi quelques manques, notamment en matière de mesures à prendre pour « donner aux consommateurs et à la communauté des chercheurs les moyens d'agir[24] ».

En amont des élections européennes de 2019, l'UE a pris des mesures additionnelles pour lutter contre le risque de manipulations de l'information à des fins d'ingérence, incluant notamment le « paquet électoral » annoncé par le président Juncker dans son discours de 2018 sur l'état de l'Union. Pendant la campagne, ont été relevées « des preuves de comportements non authentiques coordonnés visant à diffuser sur les plateformes en ligne, y compris au moyen de logiciels robots et de faux comptes, du contenu de nature à semer la division[25] ». Cependant, les mesures prises par la société civile, notamment les journalistes et vérificateurs de fait, les plateformes numériques, les autorités nationales et enfin les institutions européennes, ont maintenu ces tentatives en deçà d'un seuil de nuisance et, globalement, les élections européennes se sont bien passées. Au début de l'année 2020, la Commission envisage une réglementation contre la désinformation, « particulièrement quand de la désinformation coordonnée sur des plateformes tech peut poser des problèmes de sécurité[26] ».

Enfin, dans le cadre européen il faut aussi souligner l'importance du centre européen d'excellence contre les menaces hybrides de Helsinki (Hybrid CoE), créé en 2017, et qui constitue un hub de ressources sur le sujet, entretenant des réseaux de chercheurs, organisant des séminaires, et produisant régulièrement des publications.

Deuxièmement, un autre acteur multilatéral majeur est l'OTAN. Confrontée aux opérations informationnelles soviétiques durant la guerre froide, l'Alliance reste aujourd'hui principalement préoccupée par les menaces provenant de Russie, même si, plus récemment, elle s'est

intéressée aussi et de manière croissante à la Chine. De fait, l'OTAN est l'une des principales cibles de la désinformation et doit faire face chaque jour à un grand nombre de nouvelles fausses ou biaisées la concernant. Elles visent principalement ses intentions, présentées comme hégémoniques et agressives, son expansion et le volume de ses troupes, notamment celles déployées dans les États baltes et la Pologne, ou encore les crimes que commettraient ses soldats.

Deux acteurs majeurs en son sein sont chargés de répondre à ces attaques et plus largement d'étudier les manipulations de l'information. D'une part, la Division Diplomatie publique (PDD) du secrétariat international, à Bruxelles, qui produit régulièrement des réfutations des accusations russes, notamment sur une page dédiée du site Internet répondant aux principaux « mythes ». La PDD joue également un rôle de coordination entre les différentes structures de l'organisation et entre les Alliés. D'autre part, le centre d'excellence de l'OTAN sur la communication stratégique de Riga (NATO StratCom COE), créé en 2014, publie un grand nombre d'analyses et organise chaque année un « StratCom Summit » sur ces questions, qui est l'un des moments importants de partage et d'échange d'informations entre acteurs étatiques et non étatiques du monde entier. Certains pays asiatiques, notamment Singapour, sont de plus en plus investis dans ces événements traditionnellement « euratlantiques », car il y a en Asie une inquiétude croissante que la Chine prenne progressivement le chemin de la Russie, c'est-à-dire adopte des tactiques plus agressives[27].

Troisièmement, depuis 2018, le G7 dispose d'un « mécanisme de réaction rapide », coordonné par le Canada, qui permet de faire circuler l'information rapidement entre les pays du G7. Les personnes ressources de chaque État se connaissent et se voient régulièrement, et l'unité de coordination du ministère canadien des Affaires globales collecte et partage un grand nombre d'informations pertinentes, notamment des publications et

des événements. En termes d'accès à l'information, c'est un progrès important.

Les think tanks, passeurs d'idées

La troisième couche de la coopération internationale est celle des think tanks, acteurs non étatiques mais souvent au moins en partie financés par des États et ayant dans leurs équipes du personnel passé par des ministères, des agences ou services de l'État dans les domaines de la défense et de la sécurité, ou qui y sont encore tout en étant détachés à « l'extérieur ». Dans la zone grise entre deux mondes, ils ont à la fois l'accès à des ressources et à des informations et la capacité de les diffuser plus librement. Ils organisent régulièrement des séminaires plus ou moins fermés, dont des « tracks 1.5 », c'est-à-dire des rencontres associant officiels et société civile. Ce mélange des genres, cette fécondation croisée, permet aux officiels de « s'aérer », de récolter des idées « en dehors de la boîte », et aux membres de la société civile de mieux comprendre comment les États travaillent et d'espérer pouvoir peut-être les influencer. Parmi les rencontres connues de ce genre, on peut citer celles qu'organise le DFRLab d'Atlantic Council à Washington et à Bruxelles et celles du Centre d'excellence pour la sécurité nationale (CENS) de la S. Rajaratnam School of International Studies (RSIS) à Singapour – qui présente l'avantage de croiser les perspectives géographiques, notamment euratlantique et asiatique.

Les think tanks américains, en particulier Graphika (Camille François, Ben Nimmo), l'Atlantic Council (DFRLab), la Brookings (Alina Polyakova, désormais présidente de CEPA) et le GMF (Laura Rosenberger), produisent une part substantielle de la recherche « opérationnalisable » sur les manipulations de l'information, en lien avec les décideurs politiques mais aussi les plateformes numériques, notamment Twitter, Facebook et Google qui, de façon croissante, participent à ces activités.

L’implication de la société civile

Quelles que soient les mesures décrites dans les pages précédentes, mises en place par les États, le degré de résilience d’une société, sa capacité de résistance aux manipulations de l’information, dépend d’abord et avant tout de la mobilisation de ses citoyens. Ce sont eux qui sont en première ligne et notamment les journalistes : outre qu’ils ont tous la responsabilité de fournir des informations fiables et sincères, certains se sont spécialisés dans la chasse aux trolls et autres réseaux d’influence, et d’autres travaillent à améliorer les standards journalistiques. Sont également importants les vérificateurs de faits, qui sont souvent mais pas nécessairement des journalistes. Tous ne sont pas récents (l’américain Snopes qui est l’un des plus connus existe depuis 1994) mais ils se sont multipliés dans les années 2010, partout dans le monde, comme un indicateur supplémentaire de la prise de conscience à l’œuvre. Certains d’entre eux sont opérés par des médias connus, qui en plus de produire des informations s’occupent de plus en plus de les vérifier (AFP Fact Check, Reality Check de la BBC, Decodex du *Monde*, CheckNews de *Libération*, etc.). Mais il n’y a pas que les médias reconnus : de nombreux sites diffusant des nouvelles fausses ou biaisées prétendent eux-mêmes faire du *fact-checking*. L’Institut Poynter a donc créé en 2015 un International Fact-Checking Network et a adopté un « code » de principes communs pour garantir une vérification transparente et non partisane. Les vérificateurs « approuvés » par Poynter sont censés satisfaire ces critères méthodologiques.

Il y a également des initiatives normatives – labels, index et autres classements – permettant de distinguer les sources d’information fiables des autres. Certains ont défendu des classements « négatifs » (un classement international de la désinformation sur le modèle de ceux de Freedom House sur la liberté de la presse et de Transparency International pour la corruption)[28] ou au contraire des classements « positifs » ou une forme de

certification, comme l'initiative pour la confiance dans le journalisme (*Journalism Trust Initiative*) de Reporters sans frontières (RSF) qui entend « renverser la logique en donnant un avantage réel à tous ceux qui produisent des informations fiables, quel que soit leur statut[29] », avec l'objectif que les plateformes numériques attribuent une « prime » à la qualité dans leurs algorithmes et leur accordent donc une visibilité accrue.

Il faut aussi mentionner des initiatives citoyennes comme le phénomène dit des « elfes » (qui chassent, identifient et exposent les « trolls »), originaire de Lituanie et dont se revendiquent des milliers d'internautes essentiellement mais pas seulement en Europe centrale, orientale et nordique.

Enfin, les plateformes numériques elles-mêmes, qui ont été longtemps réticentes à reconnaître le problème, ont été contraintes à réagir. Le tournant de la coopération date de 2018, année durant laquelle elles ont commencé à partager des informations (Reddit en avril sur 944 comptes liés à l'Internet Research Agency [IRA] russe, Facebook en juillet au sujet d'une autre opération de l'IRA, Twitter en octobre sur 9 millions de tweets également attribués à l'IRA, etc.)[30]. Elles publient depuis des documents pédagogiques, comme par exemple *How Google Fights Disinformation* en février 2019, et rendent des comptes à la commission européenne dans le cadre du Code des bonnes pratiques contre la désinformation. Ces plateformes – certaines plus que d'autres – ont aussi pris l'habitude de partager des informations (pages, comptes concernés) avec certains chercheurs et analystes avec lesquels ils ont développé une relation de confiance, avant des *takedowns*, c'est-à-dire des suppressions massives de comptes[31]. Ces informations ont notamment alimenté les études de DFRLab et Graphika ces dernières années. Les plateformes consacrent désormais des moyens importants à la détection et à la suppression des manipulations de l'information sur leurs sites. À la conférence de sécurité de Munich en février 2020, Marc Zuckerberg a ainsi rappelé qu'à Facebook

35 000 personnes scrutaient la plateforme pour détecter des contenus problématiques et que, avec l'aide de l'intelligence artificielle, plus d'un million de faux comptes étaient supprimés chaque jour.

Les limites des mesures prises

L'ensemble des mesures présentées dans les pages précédentes peut sembler impressionnant. Il est indéniable qu'en l'espace de quelques années, la prise de conscience a été réelle et que les États, les organisations internationales, la société civile et même les plateformes numériques ont fait d'importants progrès dans la lutte contre les manipulations de l'information. Les défis restent toutefois considérables pour les raisons suivantes.

Premièrement, la vérification des faits est nécessaire mais insuffisante, pour au moins deux raisons. La première est que son efficacité est discutée. De nature corrective, elle est par définition *post facto,* elle arrive quand le mal est fait sans pouvoir effacer l'impact psychologique de l'information fausse ou biaisée. En outre, les études montrent que le cerveau humain est résistant à la correction et que la plupart des gens continuent de diffuser une information dont ils reconnaissent la fausseté. Et la correction peine à atteindre sa cible à cause d'une sorte de parallélisme des audiences, les personnes étant les plus susceptibles de lire des fausses nouvelles sur des sites douteux et d'être convaincues par elles n'étant en général pas les mêmes qui fréquentent les sites sérieux vérifiant les faits[32].

La deuxième raison est que ce qui compte n'est pas tant les faits que les histoires. Peu importe au fond que nous ayons raison : tant que nos adversaires auront de meilleures histoires, ils gagneront. Corriger de fausses informations n'empêchera pas qu'elles soient propagées, parce que ce qu'une certaine frange de la population recherche ce sont de « bonnes

histoires », qu'elles soient vraies ou pas. Comme l'explique bien Ben Nimmo, nous ne sommes pas tant dans une « guerre de l'information » (*information warfare*) que dans une « guerre de récit » (*narrative warfare*). De ce point de vue, corriger une fausse information ne suffit pas, il faut réussir à imposer un autre récit, à raconter une bonne histoire. Laquelle ? Celle de l'attaque, répond Nimmo. C'est ce qui a fonctionné dans le cas des « Macron Leaks » : quelques analyses en temps réel ont permis de réorienter l'attention de l'opinion publique qui s'intéressait moins au contenu des « leaks » qu'à l'origine de l'attaque et aux liens que ces mystérieux acteurs pouvaient entretenir avec un parti politique français ou des puissances étrangères. Et cela était déjà une victoire[33].

Deuxièmement, il est indéniable que la lutte contre les manipulations de l'information peut constituer une menace pour les valeurs démocratiques et libérales, en particulier la liberté d'expression. Le fait que des mesures apparemment similaires soient prises dans des démocraties libérales et des autocraties en est la preuve. Pour que les premières maintiennent un équilibre sain entre sécurité et liberté, qui est au cœur du contrat social, et se préservent de la comparaison avec les régimes autoritaires, elles doivent adopter un principe directeur selon lequel l'État n'est pas et ne doit pas être la première ligne de défense contre les manipulations de l'information : ce sont les citoyens, la société civile, en particulier les journalistes, les vérificateurs de faits et les chercheurs, qui le sont. C'est pourquoi la première des recommandations aux États dans notre rapport de 2018 était d'« avoir une empreinte légère[34] » – approche notamment adoptée dans le plan canadien présenté en janvier 2019, qui ne présume pas que l'État doit protéger des citoyens passifs, mais veut les former pour leur donner les moyens de détecter eux-mêmes les manipulations.

Troisièmement, les vertus de la transversalité sont désormais reconnues – il est évident pour tout le monde que, pour se défendre contre les manipulations de l'information, il faut faire travailler ensemble des services

voire des ministères différents –, mais toutes les cultures administratives n'y sont pas aussi réceptives. Certains pays (scandinaves, baltes, Canada) y parviennent mieux que d'autres dont la bureaucratie est plus lourde et encore très « ensilotée », avec parfois des rivalités interservices qui paralysent l'action. Tous n'ont pas la souplesse de pouvoir créer un Centre pour la politique numérique internationale comme celui du ministère canadien des Affaires mondiales, une équipe unique mêlant analystes politiques et « geeks » spécialistes des réseaux sociaux, un modèle du genre.

Quatrièmement, beaucoup d'États se focalisent sur les élections et on peut le comprendre, non seulement parce qu'elles sont l'une des incarnations de la démocratie (on doit donc les protéger au même titre que les « infrastructures critiques » qui permettent à nos sociétés de fonctionner : électricité, ponts, réseau ferré, télécommunications, hôpitaux, etc.) mais aussi parce qu'il est consensuel et bipartisan de vouloir les protéger. Néanmoins, on ne doit pas perdre de vue que les attaques – qu'elles soient cyber ou informationnelles – sont quotidiennes. Les mesures prises ne peuvent donc pas être limitées aux périodes électorales.

Cinquièmement et de la même manière, beaucoup d'États se focalisent sur l'ingérence, c'est-à-dire l'intervention étrangère, les menaces « exogènes ». Or, tous les praticiens de la lutte contre les manipulations de l'information le constatent : il n'est pas toujours facile – il est même souvent difficile et parfois impossible – de distinguer entre une manipulation d'origine « étrangère » (qu'on peut donc appeler une ingérence) et une manipulation d'origine intérieure. C'est d'autant plus difficile que nos adversaires jouent sur l'ambiguïté, en ayant recours à des proxies non étatiques, en s'appuyant sur des opérateurs nationaux. Les États sont assez démunis car ce ne sont généralement pas les mêmes services qui luttent contre les menaces extérieures et contre les menaces intérieures : l'ambiguïté de la menace implique donc la transversalité de la défense. Elle

nous force à faire tomber les barrières entre services, à faire davantage circuler l'information, ce qui n'est pas dans les habitudes de toutes les bureaucraties.

Sixièmement, à l'échelle européenne, l'organisation de la réponse du SEAE en trois équipes géographiques très déséquilibrées – le front « Est », c'est-à-dire russe, concentrant l'essentiel des moyens – ne convainc pas tous les pays, notamment ceux qui s'estiment à un carrefour entre l'Est et le Sud et/ou défendent une vision à 360°. La focalisation explicite sur la Russie, et demain peut-être aussi sur la Chine, dans tous les cas sur une menace spécifique, peut contribuer à diviser les États européens entre ceux qui assument cette opposition et les autres qui ne veulent pas apparaître « anti-Russes » ou, demain, « anti-Chinois ». En outre, la logique géographique a ses limites : les Russes, par exemple, sont très actifs en Afrique, y compris contre les intérêts européens[35]. L'« Est » est aussi au « Sud » et réciproquement. Plutôt qu'avoir trois équipes géographiques déséquilibrées, on pourrait donc imaginer un seul service luttant non pas contre telle ou telle menace étatique identifiée mais contre les manipulations de l'information d'où qu'elles viennent, y compris d'ailleurs d'acteurs non étatiques[36].

Septièmement, les formats de coopération existants (UE, OTAN, G7) sont utiles mais imparfaits, trop larges ou trop étroits, car créés pour autre chose, et dans tous les cas trop hétérogènes, les positions sur la question de savoir si les manipulations de l'information constituent une menace sérieuse étant perçues en fonction des intérêts de chacun et en particulier des relations que ces États ont ou souhaitent avoir avec ceux généralement présentés comme les principales menaces en la matière, à savoir la Russie et la Chine. Les divergences sont donc nombreuses, avec parfois des obstructions caractérisées, ce qui non seulement rend les décisions plus lentes et moins efficaces mais peut aussi parfois susciter un climat de méfiance entre les membres. C'est pourquoi se multiplient les appels à la

constitution plus ou moins formelle d'une alliance *ad hoc* d'États démocratiques, partageant les mêmes valeurs et les mêmes préoccupations, pour partager de bonnes pratiques et formuler des demandes conjointes, notamment aux plateformes numériques[37].

Huitièmement, les plateformes numériques, très critiquées, ont fait des progrès importants en matière de partage d'information ces dernières années. On ne peut plus leur reprocher de ne rien faire, comme c'était sans doute le cas à une époque. On peut toutefois exiger qu'elles fassent toujours davantage, et surtout qu'elles fassent preuve de davantage de transparence quant aux mesures prises. Lorsque Facebook quelques jours avant un *takedown* en donne la primeur à Graphika, par exemple, il leur communique les pages ou les comptes concernés avant de les supprimer au motif qu'ils sont liés au renseignement militaire russe par exemple[38], mais Facebook ne dit pas comment ils sont arrivés à cette conclusion. La communauté des chercheurs doit donc les croire sur parole, ou développer des moyens propres de confirmer – ou d'infirmer – cette attribution[39]. Bien entendu, le partage d'informations aussi sensibles que celles ayant permis l'attribution reviendrait à exposer des méthodes de détection, ce qui profiterait aux attaquants qui trouveraient, la prochaine fois, le moyen de les contourner. La question est donc celle de savoir si les plateformes numériques pourraient développer des moyens de partager des informations confidentielles (et devant le rester) avec des gouvernements mais aussi quelques chercheurs de confiance, en distinguant plusieurs niveaux d'accès.

Pour aller plus loin :

COMMISSION EUROPÉENNE, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, intitulée « Lutter contre la désinformation en ligne : une approche européenne », 26 avril 2018.

Chambre Des Communes Du Royaume-Uni, Comité Pour Les Médias, Le Sport Et La Culture, *Disinformation and « Fake News ». Final Report*, 14 février 2019. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf.

Jeangène Vilmer Jean-Baptiste, Escorcia Alexandre, Guillaume Marine, Herrera Janaina, *Les Manipulations de l'information : un défi pour nos démocraties*, rapport du Centre d'analyse, de prévision et de stratégie (CAPS) du ministère de l'Europe et des Affaires étrangères et de l'Institut de recherche stratégique de l'École militaire (IRSEM) du ministère des Armées, Paris, août 2018.

Jeangène Vilmer Jean-Baptiste, *The Macron Leaks Operation : A Post-Mortem*, Paris/Washington DC, IRSEM/Atlantic Council, 2019.

Jeangène Vilmer Jean-Baptiste, Charon Paul, « Russia as a hurricane, China as climate change : Different ways of information warfare », *War on the Rocks*, 21 janvier 2020.

Pamment James, *The EU's Role in Fighting Disinformation : Taking Back The Initiative*, Carnegie Endowment for International Peace, 15 juillet 2020.

Rapport du comité d'étude singapourien sur les fausses informations délibérées en ligne (*Deliberate Online Falsehoods*). https://www.rajahtannasia.com/media/pdf/Exec_Summary_Rpt_on_Deliberate_Online_Falsehoods.pdf.

FOCUS 5

L’OTAN et la guerre de l’information

Commissaire principal Pascal Brangetto

À la suite des cyberattaques qui ont touché l’Estonie en 2007, l’OTAN s’est emparée du sujet cyber[1]. Dans la perspective d’être toujours en mesure de respecter les clauses du contrat de sécurité qui lie ses membres, elle s’est dotée dès 2010 d’un organe capable de penser de façon prospective les nouvelles menaces, appelé Division des défis de sécurité émergents (Emerging Security Challenges Division). Elle a ainsi su mener une réflexion en parallèle des États et élaborer une doctrine. Définie en 2011, celle-ci fixe les règles de la gouvernance du cyber en son sein[2].

L’OTAN trace une ligne de partage entre son organisation politico-militaire et son organisation opérationnelle. Elle dispose en tête de chaîne d’un comité de cyberdéfense qui délègue au Bureau de gestion de la cyberdéfense (Cyber Defence Management Board) la coordination des travaux relatifs au cyber au sein de l’organisation. Le commandement allié de la transformation (ACT), basé à Norfolk aux États-Unis, traite les questions de doctrine cyber sur le plan opérationnel. L’ACT a « sous-traité » une partie de ses responsabilités en la matière au centre d’excellence de cyberdéfense (NATO CCDCOE) de Tallinn en Estonie qui est

étroitement lié au commandement intégré de l'OTAN en raison du tropisme otanien de l'Estonie, même s'il n'en fait pas formellement partie.

La doctrine cyber de l'OTAN

En 2011, l'OTAN s'est assigné deux responsabilités distinctes en matière de cyberdéfense : renforcer la cyberdéfense collective et assurer la défense de ses propres réseaux. La posture de l'OTAN sur la cyberdéfense demeure ainsi purement défensive car les États ne sont pas prêts à renoncer à leur souveraineté dans ce domaine[3]. Il y a également un intérêt bien compris de l'OTAN à s'engager dans cette démarche compte tenu des mises en cause de l'organisation[4].

La défense collective dans le cyberespace

La reconnaissance en 2013 par le groupe des experts des Nations unies de l'applicabilité du droit international au cyberespace a été centrale dans la définition d'une doctrine cohérente. La déclaration du sommet du Pays de Galles en 2014 qui en découle constitue la pierre angulaire de la doctrine cyber de l'OTAN[5]. Il y a une dimension éminemment politique et stratégique dans l'affirmation qu'une cyberattaque[6], par sa gravité et ses effets, peut atteindre le seuil d'une agression armée au sens de l'article 51 de la Charte des Nations unies. Cet article définit le droit à la légitime défense dont dérive le principe de défense collective érigé par l'article 5 du traité de Washington. La réflexion de l'OTAN, sur ce sujet, a été nourrie par les travaux du NATO CCDCOE, en particulier les *Manuels de Tallinn* qui posent les bases de l'applicabilité du droit international humanitaire au cyberespace[7]. Le succès de ces publications réside dans l'originalité de leur

initiative puisqu'elle émane d'une organisation internationale ; il tient aussi à la maturité des positions et des interprétations de droit international exprimées.

La protection des réseaux de l'OTAN

« La responsabilité fondamentale de l'OTAN en matière de cyberdéfense est de défendre ses propres réseaux. » Cette mission, assez banale en définitive, s'apparente aux responsabilités que l'on pourrait voir confier à une équipe chargée de répondre en urgence à un problème informatique (Computer Emergency Response Team, CERT) au sein d'une grande entreprise ou d'une collectivité. Le NCIRC (NATO Computer Incident Response Capability) est l'organe chargé de veiller à la sécurité des différents réseaux de l'OTAN, en particulier des réseaux de communication et de transmission interopérables avec les réseaux des États membres.

L'OTAN s'envisage également comme un facilitateur dans le domaine cyber au travers d'initiatives telles que le *cyber defence pledge* adopté en 2016. Il est demandé aux États de s'engager à respecter un niveau minimal d'exigences techniques et procédurales dans la mise en œuvre d'une stratégie de cybersécurité, d'améliorer la coordination ou le partage de l'information. En effet, il convient de souligner – en particulier dans le domaine de la cyberdéfense – que la force d'une alliance repose sur la robustesse de son maillon le plus faible[8].

La préparation aux guerres de l'information

Le conflit en Ukraine en 2014 n'a pas donné lieu à des cyberattaques significatives, comme on aurait pu s'y attendre. En revanche, il a suscité des situations conduisant à une guerre de l'information[9]. Cet effort a visé, pendant et après la phase la plus active des hostilités, à façonner

l’environnement informationnel des individus. Ici la frontière entre les opérations dites « cyber » qui sont par nature techniques et les opérations d’influence ou psychologiques est difficile à tracer[10]. Cette situation a accéléré la mise en place de structures dédiées à l’étude et à la conception de techniques visant à contrer les effets d’attaques sur l’information à grande échelle. La création à Riga en Lettonie d’un centre d’excellence consacré à la communication stratégique (NATO STRATCOM CoE, centre d’excellence en communication stratégique) témoigne de l’importance grandissante de la maîtrise du récit (*narrative*) dans le cadre de conflits où la désinformation joue un rôle central.

L’intégration du cyber dans les exercices de l’OTAN

En 2016, lors du sommet de Varsovie, le cyberespace a été reconnu comme un domaine d’opérations à part entière[11]. L’OTAN a très tôt compris l’intérêt d’inclure des aspects cyber dans ses exercices au profit de l’ensemble des États membres. Les exercices de l’OTAN comportant des éléments cyber peuvent se classer selon trois catégories.

Les exercices classiques

Les exercices classiques incluent un ou plusieurs scénarios (*storylines)* impliquant une menace cyber. Ces exercices de grande envergure avec déploiement réel de troupes sur des terrains de manœuvre sont particulièrement exigeants. Il s’agit ici de garantir la sécurité des réseaux déployés sur un théâtre d’opérations (réseau OTAN, réseau national,

systèmes d’armes souvent adossés à des systèmes d’exploitation OS (Windows, Linus), également employés dans le civil).

Les exercices proprement cyber

Les exercices principalement axés sur le cyber combinent des aspects institutionnels et techniques. L’objectif dans ce cadre-là est de tester les chaînes de commandement et de constater comment se répartissent les attributions et responsabilités. C’est l’occasion pour l’échelon national de vérifier la robustesse du dispositif mis en place et d’observer comment réagissent les différentes parties prenantes. Il peut également s’agir de scénarios impliquant des tiers externes, fournisseurs d’OS, fabricants de terminaux. Ces exercices peuvent être également l’occasion de tester des outils de connaissance de la situation (*situational awareness*) ainsi que des plateformes d’échange d’informations (*information sharing*). L’exercice Cyber Coalition qui se tient chaque année en Estonie est le plus important exercice de ce type organisé par l’OTAN. Enfin, des exercices calqués sur le modèle du *serious gaming* se multiplient. Il s’agit, le plus souvent, d’exercices sur table (*tabletop exercise*) avec des simulations de prise de décision.

Les exercices de défi technique

Le troisième type d’exercice repose sur des défis techniques que des spécialistes se lancent et tentent de remporter. Il rappelle les jeux de la culture du joueur (*gamer*) propre aux informaticiens. Il n’est pas toujours simple d’associer la dimension institutionnelle d’une organisation internationale militaire à celle du *gamer*. À ce titre, le NATO CCDCOE se donne pour mission d’entraîner des unités spécialisées dans la lutte informatique en faisant coexister ces deux approches distinctes. Le centre

de Tallinn propose deux exercices défensifs « Boucliers verrouillés » (*Locked Shields*) et les exercices offensifs « Fer croisé » (*Crossed Swords*)[12] à grande échelle qui permettent de faire « jouer » plusieurs équipes nationales. Il s'agit principalement de tester les défenses d'un système d'informations sur le modèle de l'exercice *Eligible Receiver*[13] dans un contexte plus défini que ne le ferait une équipe chargée de pénétrer un réseau dans le cadre d'un audit de sécurité (*pentesters* suivant l'expression consacrée).

La clé de la réussite de ces exercices techniques est de disposer d'infrastructures adaptées pour faire vivre à grande échelle des incidents cyber-réalistes, tout en faisant participer un grand nombre d'équipes de « joueurs ». Les scénarios de ces exercices s'attachent, par exemple, à mettre des équipes de défense en difficulté face à une équipe d'adversaires, appelée « l'équipe rouge » (*red team*) non sans allusion à la Russie. Dans le cas de l'exercice *Locked Shields*, les forces armées estoniennes mettent à disposition du NATO CCDCOE leur champ de tir virtuel (*cyber range*). Par le biais de plusieurs serveurs, le *cyber range* permet de générer un trafic équivalent à celui d'Internet, de simuler des attaques (DDOS) et de mettre en œuvre des solutions défensives (*sinkhole*).

CHAPITRE 17

La régulation pour contrer les manipulations de l’information en ligne : l’impossible consensus international ?

Frédérick Douzet et Aude Géry

Le piratage des serveurs du Comité national démocrate (DNC) et la publication des e-mails internes du parti au cours de la campagne présidentielle de 2016 ont pris l’administration américaine complètement par surprise. Redoutant une vaste cyberopération destinée à porter atteinte à l’intégrité du processus électoral, le gouvernement a pris conscience de l’ampleur des vulnérabilités d’un scrutin reposant sur des machines à voter et des registres électoraux peu sécurisés. C’est pourtant sur le plan essentiellement informationnel que l’opération d’ingérence – attribuée par la Maison Blanche à la Russie – s’est déroulée, exploitant une faille bien plus grande encore : la polarisation politique de la société américaine et le ressentiment populaire à l’égard de l’establishment[1].

Ce type de manipulations de l’information n’appartient pas au registre classique des cyberopérations offensives et n’avait jusqu’ici pas été débattu dans le cadre des efforts de régulation du cyberespace. Cet angle mort dans

l’analyse de la menace s’explique avant tout par une vision très occidentale et techno-centrée du cyberespace que d’autres États, à commencer par la Chine et la Russie, se représentent avant tout comme un espace informationnel et une menace susceptible de porter atteinte à la stabilité de leur régime politique et de leurs sociétés.

Or c’est bien à ce type de menace que sont désormais confrontées les démocraties occidentales. Elles découvrent à leurs dépens la possibilité – décuplée par les réseaux sociaux – pour des acteurs politiques de manipuler à grande échelle l’opinion publique et dévoyer ainsi le processus électoral, en instrumentalisant la liberté d’expression comme levier de déstabilisation dans un contexte de crise de confiance dans les institutions et de montée des populismes.

Dès lors, les initiatives se multiplient pour juguler la menace et tenter de réguler les activités en ligne, au niveau national mais aussi international et du secteur privé. Ces initiatives dispersées reflètent l’étendue et la complexité du spectre des manipulations de l’information, et la grande confusion sémantique qui règne.

Camille François propose un cadre d’analyse articulé autour des trois principaux vecteurs de la manipulation virale de l’information afin d’avancer des pistes de régulation pour les législateurs et des stratégies de réponse pour le secteur privé[2]. Son ABC de la désinformation distingue : A) les acteurs malveillants (*Manipulative Actors*) qui s’engagent délibérément dans des campagnes de manipulation en ligne en cherchant à masquer leur identité et leurs intentions ; B) les comportements trompeurs (*Deceptive Behavior*), vecteur principal des campagnes de désinformation qui comprennent une grande diversité de techniques pour amplifier la portée, la viralité et l’impact des campagnes ; C) les contenus malveillants (*Harmful Content*), très présents dans les campagnes électorales, critère le plus subjectif.

Ce chapitre vise à expliquer la diversité et la nature des initiatives mises en place à l'échelle internationale pour lutter contre la désinformation, en s'appuyant sur le cadre d'analyse développé par Camille François. Nous montrerons dans un premier temps que la lutte contre les acteurs malveillants (A. *Manipulative Actors*) peut s'appuyer sur des règles existantes du droit international mais aussi sur la mise en œuvre des chartes des utilisateurs des plateformes, à l'instar de la lutte contre la propagande djihadiste. La lutte contre les comportements trompeurs (B. *Deceptive Behaviors*) reste pour l'instant le domaine presque réservé des plateformes, mais pourrait faire l'objet d'une régulation internationale, et nécessite une meilleure coopération public-privé. La régulation du contenu malveillant (C. *Harmful Content*), enfin, se heurte à de sérieuses limites de définition de l'objet, mais aussi et surtout de respect du droit international, notamment des droits de l'homme, limitant la portée des initiatives de régulation et la capacité des États à atteindre un consensus.

Neutraliser les acteurs malveillants

Lorsque l'on s'interroge sur les moyens offerts pour réguler les manipulations de l'information – et réagir –, on peut tout d'abord s'appuyer sur le droit international, ce que l'administration Obama a prudemment commencé à faire en dénonçant l'ingérence russe dans l'élection présidentielle américaine en 2016[3].

Un recours limité au droit international

La mise en œuvre du principe de non-intervention dans le cadre des manipulations de l'information n'est pas aisée. Il faut tout d'abord identifier

et attribuer juridiquement l'opération à un État. Il faut ensuite qualifier l'opération, c'est-à-dire établir l'élément coercitif de l'intervention, entendu comme le fait de vouloir contraindre un État à agir d'une façon déterminée, et prouver que l'opération portait sur un sujet relevant du domaine réservé de l'État. Les élections au sein d'un État relèvent sans aucun doute de son domaine réservé. Toute la difficulté réside dans l'identification de l'élément coercitif dans le cadre des manipulations de l'information dont les effets, contrairement aux cyberopérations contre l'infrastructure électorale (machines à voter, données électorales), relèvent de l'influence et sont difficilement mesurables[4].

Le principe de non-intervention renvoie aux débats plus larges sur l'intervention indirecte dans les affaires intérieures dont la définition ne fait pas l'objet d'un consensus en droit international, particulièrement pour ce qui relève des actions politiques et économiques. De plus, il est à double tranchant car il est aussi l'instrument privilégié par les États autoritaires pour défendre leur légitimité à contrôler les contenus en ligne et pratiquer une censure institutionnalisée. Ainsi, les États mêmes qui cherchent désormais les moyens juridiques de contrer les manipulations de l'information de la part d'acteurs étrangers sont confrontés, pour justifier leur action, à des choix d'interprétation du droit international contre lesquels ils se sont battus pendant des années.

In fine, la mise en œuvre du droit international en la matière se heurte aux mêmes difficultés que dans le cadre de la lutte contre les cyberattaques, car elle repose sur les mêmes piliers : la capacité de détecter les opérations, domaine qui est nouveau et complexe pour les États focalisés jusqu'à récemment sur les menaces techniques et qui ouvre un champ de recherches innovantes ; la capacité à attribuer juridiquement l'opération à un État ; la capacité à qualifier l'opération au regard du droit international ; et enfin, la capacité à trouver des leviers pour réagir aux actes illicites, et plus largement pour empêcher et dissuader l'acteur malveillant d'agir, dans le

respect du droit international (perturbation de l'adversaire, réponse proportionnée, etc.).

Or ces acteurs se cachent derrière des proxies**,** compliquant leur identification. Ils peuvent être des agents d'État, des mercenaires, de simples hackers patriotes agissant de leur propre initiative ou encore des individus cherchant à générer un profit à partir de sites de désinformation[5]. À l'image des attaques persistantes (APT), ces *Advanced Persistent Manipulators* (APM)[6] sont difficiles à détecter et à stopper : ils poursuivent leurs cibles et leur mission coûte que coûte et ne se laisseront pas décourager par une simple fermeture de comptes. Ils présentent ainsi la même détermination, agilité et capacité d'adaptation que les propagandistes de Daech[7].

Les difficultés d'attribution et de qualification de l'attaque restent ainsi un frein important à la mobilisation du droit international, qui s'avère peu efficace pour contrer le phénomène et dissuader les acteurs. D'où la nécessité d'initiatives complémentaires, auxquelles les plateformes du Web se sont essayées.

L'engagement prudent des plateformes du Web

La question est cependant délicate pour les plateformes, détournées de leur usage par les acteurs malveillants pour mener leurs opérations. Ces entreprises opèrent au niveau mondial et tout leur modèle économique repose sur la confiance des utilisateurs. La décision de bannir des acteurs va à l'encontre de leur culture, leur idéologie, leurs compétences et leurs intérêts économiques.

Elles y ont toutefois été amenées dans le contexte de la montée en puissance du terrorisme dans les années 2010, sous une pression publique et politique importante. La prise de conscience de leur pouvoir, et donc de leur responsabilité, dans le phénomène de radicalisation en ligne s'est faite

progressivement. Elle a abouti à des solutions privilégiant le recours au signalement par les utilisateurs et les services gouvernementaux de comptes et contenus contrevenant clairement à leur charte des utilisateurs (*terms of service*) qui interdit les propos incitant à la violence. La suppression de ces comptes et contenus s'est révélée d'une efficacité relative. Elle a néanmoins permis de limiter et de ralentir la propagation de contenus malveillants.

Or la question est beaucoup plus compliquée dans le contexte de l'influence. Elle ne fait pas l'objet d'une définition claire et cohérente dans les chartes d'utilisateurs des plateformes qui tentent d'aborder la question de manière indirecte, sans interdire explicitement la manipulation dissimulée de leurs services par des gouvernements à des fins d'influence. Et le ciblage des acteurs peut s'avérer un terrain politiquement glissant. Par exemple, en novembre 2017, le PDG de Google annonçait le déréférencement des médias russes Russia Today et Sputnik. Au même moment se tenait le sommet de l'Internet de Wuzhen, en Chine. Vivement interpellé par un participant sur le blocage de Google et Facebook en Chine, un panéliste chinois a immédiatement brandi la nouvelle de Google en demandant ironiquement quelle pouvait bien être la différence. Une semaine après, accusé de censure par la Russie, le PDG de Google renonçait à sa décision.

Face aux difficultés d'établir des critères légitimes, Twitter a ouvert la voie en août 2019 en interdisant toute publicité émanant de médias contrôlés par les États, à la suite d'une enquête démontrant qu'un média d'État chinois avait utilisé la publicité sur Twitter pour diffuser des messages à l'encontre des manifestants de Hong Kong[8]. Mais là encore, les difficultés à catégoriser les médias en fonction de leurs sources de financement et de leurs liens avec l'État d'origine risquent de compliquer la mise en œuvre de cette décision. De plus, ces initiatives sont privées et ne sont aucunement rattachables à l'ordre juridique international. Si elles constituent une tentative de réponse de la part des plateformes, elles ne

s’inscrivent aucunement dans le cadre de la régulation internationale. Les plateformes sont en revanche beaucoup mieux armées pour lutter contre les techniques et modes de propagation qui assurent la viralité et la visibilité des contenus, en détectant les comportements problématiques. Ces mêmes limites se retrouvent toutefois dans l’approche sur les comportements.

Cibler les comportements trompeurs

Les comportements trompeurs regroupent toutes les techniques et modes opératoires permettant d’amplifier un contenu et d’augmenter de manière masquée et coordonnée la portée, la viralité et l’impact des campagnes de désinformation. Le concept englobe ainsi le recours aux outils automatisés (armées de bots) ou la ruse manuelle (achat de publicités, fermes de trolls)[9].

Le rôle-clé des plateformes en matière de détection

Les plateformes sont d’autant mieux armées pour s’attaquer à ces comportements qu’elles représentent une partie du problème. Car c’est bien sur la technologie et le modèle économique construits par les plateformes que les manipulateurs s’appuient, en les détournant de leur usage initial : facilité d’élaboration des comptes, publicité ciblée, algorithmes de recommandations, amplification des contenus populaires, facilité et rapidité de partage, etc.

Par sa dimension très technique qui s’inscrit dans le prolongement des questions de cybersécurité, l’approche par les comportements a cristallisé les efforts de lutte contre la désinformation de la part des plateformes, de

manière plutôt cohérente. Les définitions de Google et Facebook sont ainsi relativement convergentes.

Facebook évoque des « comportements coordonnés et non authentiques » définis ainsi : « On parle de comportements coordonnés et non authentiques lorsque des pages, des comptes, des personnes agissent ensemble pour tromper des personnes sur qui ils sont ou ce qu'ils font[10]. » Cette politique, qui a permis le démantèlement de *botnets* et la suppression de nombreux comptes depuis 2018, permet d'éviter le cœur du problème – le contenu des publications – en se focalisant sur la méthode.

De la même façon, dans son Livre blanc de février 2019 intitulé *Comment Google combat la désinformation*, Google identifie ces comportements trompeurs comme le vecteur principal de la désinformation sur ses plateformes, qu'il définit d'ailleurs comme : « des efforts délibérés de duper et tromper en utilisant la vitesse, l'ampleur et les technologies du Web ouvert[11] ».

Les initiatives restent toutefois fragmentées et souvent en dehors de tout cadre juridique, aussi bien entre les plateformes que parfois entre les produits au sein d'une même plateforme.

L'absence de projet de régulation internationale

De plus, dans ce domaine, la plus grande opacité règne sur les choix effectués par les plus grandes plateformes, auxquels ni les législateurs ni les utilisateurs n'ont accès. Les initiatives visant à la transparence sont rares et limitées[12] même si l'Union européenne adopte progressivement des règles en ce sens, conduisant ainsi à un début de régulation. Or ces choix ont une portée politique et démocratique majeure. Quelles sont les règles applicables ? Comment sont déterminées les priorités dans les choix de détection ? Comment les utilisateurs seront-ils informés ? Quelles sont les possibilités de recours ?

Étant donné l'enjeu, on pourrait considérer que ces règles devraient être fixées par les États. La Californie a mis en œuvre une loi expérimentale connue sous le nom de *BOT Law* pour *Bolstering Online Transparency* (renforcer la transparence en ligne). La loi « interdit à toute personne d'utiliser un bot pour communiquer ou interagir avec une autre personne en ligne en Californie[13] », mais n'impose pas d'obligation aux plateformes. À l'échelle internationale, les États auraient la possibilité de légiférer même s'il n'y a pour l'instant pas d'initiative en ce sens. Les États sont toutefois limités dans leur capacité à définir un cadre juridique pertinent aussi bien à l'égard des acteurs malveillants que des comportements trompeurs. D'une part, les techniques utilisées le sont également à d'autres fins, compliquant toute approche de régulation fondée sur le contrôle des techniques en elles-mêmes. D'autre part, ce sont les plateformes qui concentrent l'essentiel des données pertinentes pour mener les investigations, aboutissant ainsi à une « asymétrie spectaculaire d'information entre les plateformes visées par ces campagnes et le reste du monde[14] ». L'absence de partage de ces informations, malgré les enjeux démocratiques, limite donc la capacité à élaborer un cadre juridique adapté.

Enfin, les initiatives évoquées ci-dessus évitent totalement la question du contenu, qui est au cœur des campagnes, pleinement visible et sur lequel chacun peut se forger une opinion en fonction de ses propres représentations, ce qui rend sa définition – et donc sa régulation – d'autant plus problématique à l'échelle internationale.

Réguler les contenus nocifs : le consensus impossible ?

La *Déclaration conjointe sur la liberté d'expression et les « fake news », la désinformation et la propagande* des rapporteurs de plusieurs organisations régionales et internationales illustre, par son titre comme par son contenu, la difficulté à s'accorder sur une définition du phénomène et à identifier le périmètre des problématiques. Elle souligne que « le droit humain de répandre des informations et des idées n'est pas limité aux déclarations "correctes", que ce droit protège aussi les informations et les idées qui pourraient choquer, offenser et déranger, et que les interdictions en matière de désinformation pourraient violer les standards des droits de l'homme, mais que, dans le même temps, cela ne justifie pas la diffusion d'informations fausses en connaissance de cause ou en toute insouciance par des acteurs officiels ou étatiques[15] ». La subjectivité de la perception des contenus et des comportements associés à la manipulation de l'information représente ainsi le principal frein à l'élaboration d'un cadre juridique international.

Le précédent du terrorisme

La lutte contre la diffusion en ligne de contenus terroristes est le domaine dans lequel les initiatives internationales sont les plus abouties. Cela peut sembler paradoxal alors même que les propositions initiales de la Russie et de la Chine en matière de régulation du cyberespace[16] qui comprenaient le contrôle des contenus pour lutter contre le terrorisme furent jugées inacceptables par les États occidentaux en raison des potentielles atteintes aux droits de l'homme. Le contexte de menace djihadiste mondiale facilitée (*enabled)* par le Web et les réseaux sociaux a cependant ouvert une voie. La capacité à identifier des contenus jugés non désirables s'appuie ainsi sur l'identification d'un acteur (ou d'un groupe d'acteurs) dont l'action a été qualifiée de menace à la paix et à la sécurité internationales.

Prenant « *acte* de l'évolution du lien qui existe entre le terrorisme et les technologies de l'information et des communications, en particulier Internet, et de l'usage qui est fait de ces technologies pour commettre des actes de terrorisme ou faciliter leur commission, notamment pour recruter, inciter à commettre, financer et planifier de tels actes[17] », le Conseil de sécurité des Nations unies a notamment demandé au Comité contre le terrorisme d'« [é]laborer de nouvelles initiatives pour renforcer les partenariats public-privé dans la lutte contre la propagande terroriste[18] ».

Le *Cadre international global de lutte contre la propagande terroriste* rédigé par le Comité contre le terrorisme contient trois piliers, dont le deuxième et le troisième ont trait aux contenus[19]. Le deuxième pilier est le renforcement des partenariats public-privé en matière de lutte contre la propagande terroriste, leur existence étant « un élément-clé du cadre international global de lutte contre la propagande terroriste[20] ». Le troisième pilier est le développement de contre-discours et d'autres moyens de contre-propagande, notamment à travers l'éducation.

La coopération public-privé encouragée par le Conseil de sécurité s'est matérialisée dans le rapport conjoint listant les bonnes pratiques pour le secteur privé dans ce domaine, présenté par l'ONG ICT4Peace et le Comité contre le terrorisme, et dans le lancement d'une initiative conjointe appelée Tech Against Terrorism. Quelques mois plus tard, Facebook, Microsoft, Twitter et YouTube annonçaient la création du Forum Internet mondial pour lutter contre le terrorisme (GIFCT) qui a établi un partenariat avec *Tech Against Terrorism*. S'il n'est pas officiellement lié aux travaux du CTED, sa création a néanmoins été saluée par le président du Comité contre le terrorisme. Le CTED et le GIFCT collaborent dans l'élaboration des meilleures pratiques pour lutter contre les contenus à caractère terroriste.

Encouragée par d'autres instruments internationaux[21], la lutte contre la diffusion des contenus à caractère terroriste et extrémiste[22] a pris un nouvel essor avec l'adoption le 15 mai 2019, à l'initiative de la France et de la

Nouvelle-Zélande, de l'*Appel de Christchurch pour supprimer les contenus terroristes et extrémistes violents en ligne*. Pour la première fois, cinquante et un États et organisations internationales et huit fournisseurs de services en ligne s'engageaient dans un document conjoint à prendre les mesures nécessaires, dans le respect des droits de l'homme, « pour faire face au problème des contenus terroristes et extrémistes violents en ligne et prévenir les utilisations abusives de l'Internet[23] ».

Si les défis sont nombreux et que la notion même de contenu à caractère terroriste ou extrémiste ne fait pas consensus, les efforts fournis dans ce domaine illustrent la capacité des États à s'accorder, d'abord entre eux, sur l'identification de contenus et le besoin de limiter leur propagation afin d'assurer la paix et la sécurité internationales. Ils montrent également l'établissement de partenariats public-privé, y compris sur un sujet touchant au cœur de la sécurité des États. Or cette institutionnalisation de l'identification de la menace et des réponses coordonnées fait défaut dans le cas des actions informationnelles.

L'absence d'institutionnalisation internationale de la lutte contre la désinformation

À l'inverse de la diffusion d'informations à caractère terroriste ou extrémiste, il n'existe pas d'initiative internationale portant sur les actions informationnelles[24] étatiques. Au niveau régional, l'Union européenne s'est toutefois saisie de ce sujet. Ainsi, depuis 2015, elle a progressivement mis en place des unités chargées de lutter contre les manipulations de l'information[25], lancé une consultation publique sur les fausses nouvelles et la désinformation[26], créé un groupe d'experts de haut niveau sur les fausses nouvelles et la désinformation en ligne[27], adopté une communication sur la désinformation en ligne[28] et élaboré un *Code européen de bonnes pratiques contre la désinformation en ligne* présenté le 26 septembre 2018.

L’analyse des différents documents élaborés sous l’égide de l’Union européenne en matière d’actions informationnelles puis adoptés montre tout d’abord l’évolution de la perception de la menace, partant d’une approche économique – la notion de *fake news* étant attachée à la lutte contre les fausses publicités – pour aboutir à la notion de désinformation en passant par celle de fausses nouvelles. Elle illustre également une évolution de l’appréciation de la responsabilité des plateformes à travers l’adoption d’une position de plus en plus critique à leur égard[29]. Enfin, elle révèle une préférence pour l’autorégulation laissée aux mains du secteur privé à l’adoption d’obligations juridiques[30].

Le choix de l’instrument, d’ailleurs, en témoigne : un code de bonnes pratiques, c’est-à-dire un instrument non contraignant, signé par des acteurs privés et contenant des bonnes pratiques à mettre en œuvre pour lutter contre la désinformation. Il faut d’ailleurs relever que ce Code a été rédigé par les plateformes à la demande de la Commission, celle-ci ne s’étant que peu impliquée dans son élaboration. De plus, il se limite à préciser qu’il « s’applique dans le cadre de la législation en vigueur de l’Union européenne et de ses États membres ». Plus important encore, il reconnaît une responsabilité commune aux plateformes à agir contre la désinformation tout en leur laissant le choix des moyens pour y parvenir, au motif que « les différents signataires agissent différemment, avec des objectifs, des technologies et des publics différents ». Il admet donc que les bonnes pratiques identifiées pourront être mises en œuvre de façon différente, laissant ainsi une grande liberté aux plateformes. Cela illustre la difficulté pour la Commission à se saisir du sujet de la désinformation et à définir le contenu des actions qu’elle souhaite voir engager par les plateformes, difficulté renforcée par les profondes dissensions existant au sein des institutions européennes.

Au-delà du consensus européen, des définitions confuses

La lutte contre les manipulations de l'information ne fait l'objet que d'un relatif consensus au niveau européen. Peut-on espérer aller plus loin et, comme en matière de terrorisme, aboutir à une action coordonnée à l'échelle internationale ? Les velléités en la matière se heurtent à l'incapacité à définir ce contre quoi l'on veut lutter. S'agit-il des fausses nouvelles ? De la propagande ? De la désinformation ? Des manipulations de l'information ? Le titre de la *Déclaration conjointe sur la liberté d'expression et les « fake news », la désinformation et la propagande* des rapporteurs spéciaux sur la liberté d'expression (citée plus haut) est en ce sens significatif : le texte porte sur les fausses nouvelles, la désinformation et la propagande, mêlant une fois de plus le critère du contenu d'une information et celui de l'adoption d'un comportement – le fait d'utiliser un contenu à des fins déterminées – pour définir son objet.

Deux éléments permettent d'expliquer cette difficulté à s'accorder sur la façon de lutter contre les manipulations de l'information. Le premier est l'incapacité à objectiver les notions de manipulations de l'information et de désinformation illustrée par l'emploi de termes aussi divers que fausses nouvelles, désinformation, mésinformation, malinformation, déception virale, etc.[31]. Une étude des différentes définitions montre que la notion même de manipulation de l'information ne fait pas consensus. À titre d'exemple, le *Code européen de bonnes pratiques contre la désinformation en ligne* définit la désinformation suivant plusieurs critères : il s'agit d'« informations dont on peut vérifier qu'elles sont fausses ou trompeuses », a) qui sont cumulativement « créées, présentées et diffusées dans un but lucratif ou dans l'intention délibérée de tromper le public » et b) qui sont « susceptibles de causer un préjudice public », au sens où elles constituent des « menaces aux processus politiques et d'élaboration des

politiques démocratiques et aux biens publics, tels que la protection de la santé des citoyens de l'Union, l'environnement ou la sécurité ».

La *Déclaration conjointe* précitée définit quant à elle la désinformation comme les déclarations faites par des États dont ils savent ou devraient raisonnablement savoir qu'elles sont fausses (§ 2(c)). Si le critère de la finalité d'un comportement pour qualifier la désinformation est mentionné dans le préambule de la *Déclaration conjointe*, son absence dans les principes recommandés aux États est de nature à mettre l'accent sur le critère du contenu plutôt que sur celui du comportement dans la définition de la désinformation. La distinction entre les deux définitions est également marquée par le recours au critère de la vérification de la source. S'il est utilisé pour définir la désinformation dans le *Code européen de bonnes pratiques contre la désinformation en ligne*, il est en revanche un critère de définition de la propagande dans la *Déclaration conjointe*.

Ces deux exemples sont corroborés par une analyse des différentes définitions des termes employés. Une telle analyse montre que ces définitions utilisent différents critères : la nature du contenu (faux, déformé, exagéré, partiellement erroné, etc.), la finalité de l'élaboration et la diffusion du contenu (adhésion à une idéologie, dénigrement, établissement du doute dans les institutions, profit financier, etc.), les effets sur les individus et la sécurité nationale et internationale et la nature vérifiable de l'information.

À ces quatre critères utilisés alternativement ou cumulativement, il faut en ajouter un cinquième : l'identité de l'acteur à l'origine du contenu. C'est le deuxième facteur qui explique la difficulté à s'entendre sur une définition commune.

La désinformation et les manipulations de l'information sont particulièrement associées à quelques États, au premier rang desquels la Russie. Consciemment ou non, l'identité de l'acteur à l'origine du contenu et du comportement associé va influencer la qualification retenue et donc le

choix de parler d'influence, de propagande ou de manipulations de l'information. Même si les critères d'objectivation académique permettent de catégoriser ces différentes opérations, le choix des termes reste éminemment politique. Ce qui pourra être perçu comme de la propagande par un État pourra l'être comme de l'influence ou encore une manipulation de l'information par d'autres[32].

La déclaration commune des ministres de l'Intérieur du G7 du 23 avril 2018 « Défendre la démocratie – S'attaquer aux menaces étrangères » illustre le rôle du critère de l'acteur dans la qualification de la nature du problème. En effet, cette déclaration porte exclusivement sur les actions informationnelles étrangères comme menace pour la démocratie. Elle écarte ainsi tout un pan de la problématique, à savoir les manipulations de l'information par l'État sur son propre territoire. Ce choix peut certes s'expliquer par les préoccupations prioritaires des signataires de la déclaration. Il témoigne toutefois d'une approche partielle de la problématique en raison du lien pouvant exister entre une action informationnelle étrangère et son instrumentalisation, à leur profit, par des acteurs nationaux. Or le choix des États d'aborder ces questions par le biais des contenus renforce cette approche subjective de la problématique.

La liberté d'expression et les restrictions pouvant y être apportées ont de tout temps fait l'objet d'appréhensions différentes selon que l'on se place du point de vue d'un État ou d'un autre. Or toute réglementation des comportements à des fins de lutte contre les manipulations de l'information conduit nécessairement, mais pas exclusivement, à restreindre la liberté d'expression. Ce dilemme du contrôle des contenus constitue un piège dans lequel les États occidentaux ne veulent pas tomber car toute négociation internationale sur ce sujet ouvrirait la porte à l'insertion de la dimension informationnelle des technologies de l'information et des communications (TIC), demandée par la Chine et la Russie depuis des années, dans les discussions internationales sur la régulation du cyberespace.

La lutte contre les manipulations de l'information comme enjeu de sécurité internationale pourrait alors servir de justification pour légitimer un plus grand contrôle des contenus par les États. En ce sens, la création par l'Assemblée générale des Nations unies d'un comité intergouvernemental spécial d'experts à composition non limitée « ayant pour mission d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles[33] » a été dénoncée par les États occidentaux comme le moyen pour la Russie d'imposer de nouvelles restrictions à la protection des droits de l'homme au nom de la lutte contre l'utilisation des TIC à des fins criminelles[34]. Quand bien même les États occidentaux arriveraient à s'entendre sur les notions de manipulation de l'information et de désinformation, il n'est pas certain qu'ils chercheraient à aboutir à une initiative internationale dans ce domaine de crainte d'offrir de nouveaux outils de coercition et de légitimation à des États exerçant un contrôle strict de l'information.

Les limites des tentatives de régulation

Au-delà du problème de représentation et de définition de la menace, les différentes initiatives régionales ou privées relatives aux manipulations de l'information se heurtent ainsi à plusieurs limites : l'absence d'approche commune du problème, les règles du droit international en matière de limites à la liberté d'expression et une mise en œuvre effective et respectueuse des droits fondamentaux des réponses aux manipulations de l'information.

L'absence d'approche commune du problème

La première limite est liée à leur objet. Comme expliqué précédemment, la notion de manipulation de l'information ne fait l'objet d'aucun consensus et c'est la finalité d'un comportement – et non la nature même d'un contenu – qui tend à définir le champ matériel des dispositions adoptées. La définition même d'un contenu malveillant n'est pas toujours gage de cohérence. À titre d'exemple, bien que les lois françaises relatives à la lutte contre les manipulations de l'information[35] définissent les contenus visés, elles sont difficilement applicables.

En effet, en excluant les inexactitudes ou simples exagérations du champ matériel de la loi, un grand nombre d'informations souvent qualifiées de fausses nouvelles ne tombaient pas sous le coup de l'incrimination. La difficulté à qualifier les contenus et les recoupements entre les catégories laissent place à l'arbitraire pour déterminer le caractère illicite d'un contenu. Dès lors, elle constitue une menace pour la liberté d'expression.

Les contraintes du droit international

La deuxième limite porte sur leur légalité au regard du droit international. La liberté d'expression est un droit fondamental consacré par de nombreux instruments régionaux et internationaux dont l'article 19 (2) du Pacte international relatif aux droits civils et politiques adopté par l'Assemblée générale des Nations unies le 16 décembre 1966. Pour autant, le droit à la liberté d'expression n'est pas absolu. Il peut notamment être limité à des fins de « respect des droits ou de la réputation d'autrui » et de « sauvegarde de la sécurité nationale, de l'ordre public, de la santé ou de la moralité publiques » et sous réserve que les restrictions envisagées soient expressément prévues par la loi et nécessaires[36]. Au niveau régional, tant la Convention européenne des droits de l'homme (article 10) que la Charte européenne des droits fondamentaux (article 11) protègent la liberté

d’expression, un contrôle strict de la légalité des législations nationales étant opéré par les cours respectives[37]. Ce dilemme entre lutte contre les manipulations de l’information et protection de la liberté d’expression transparaît d’ailleurs dans tous les documents élaborés et les déclarations des autorités politiques et des entreprises relatives aux efforts entrepris en la matière, la recherche d’un juste équilibre étant permanente et particulièrement mise en avant[38].

Des réponses difficiles à mettre en œuvre

La troisième limite réside dans la mise en œuvre de ces différentes approches trop souvent laissée à l’initiative du secteur privé. En effet, si l’identification des meilleures pratiques et la production de rapports de transparence sont de nature à encourager une uniformisation de la lutte contre les manipulations de l’information ou des contenus illicites, la place limitée – voire l’occultation – du rôle du juge dans les engagements pris par les signataires des différents codes de conduite envoie le message d’un rôle prépondérant des plateformes dans la détermination des contenus devant être supprimés. Cela n’implique pas nécessairement que le juge est absent de toute procédure, les législations nationales pouvant prévoir la saisine du juge des référés pour faire cesser la diffusion des contenus litigieux[39].

Se pose néanmoins la question de la transparence des critères et des décisions opérées par les plateformes, ou encore des recours offerts aux citoyens pour contester le retrait de comptes et contenus jugés illicites par les plateformes. La définition même des contenus et la pression sur les plateformes peuvent conduire à une surréaction, renforcée par les délais de retrait imposés par les États. À titre d’exemple, Twitter a refusé dans un premier temps d’autoriser la diffusion de la campagne #OuiJeVote du gouvernement français pour les élections européennes au motif qu’il était incapable de mettre en œuvre les obligations énoncées dans la loi française

sur les manipulations de l'information[40]. Ce risque est explicitement nommé dans le *Code européen de bonnes pratiques contre la désinformation en ligne* qui dispose que « les signataires ne devraient pas être contraints par les gouvernements d'effacer des contenus ou des messages par ailleurs licites ou d'empêcher l'accès à ceux-ci au seul motif qu'ils sont jugés faux, pas plus qu'ils ne devraient adopter de politique volontaire en ce sens » (§ II D).

Cette situation est renforcée par les différentes définitions pouvant être adoptées par les États dans leurs législations nationales, nécessitant de la part des plateformes une agilité dans la détection des contenus et la réaction à y adopter. Cette fragmentation du contrôle des contenus risque ainsi d'augmenter la subjectivité associée à la lutte contre les contenus jugés indésirables.

Ces trois grandes limites ne doivent néanmoins pas masquer une prise de conscience des États européens et des plateformes de la nécessité de collaborer à l'élaboration d'un cadre normatif permettant de préserver la liberté d'expression tout en luttant contre des contenus et comportements considérés comme portant atteinte à la dignité des individus, à l'intégrité des processus démocratiques ou à la sécurité nationale et internationale. Ces limites interrogent toutefois sur la capacité des États à aboutir à un consensus afin de lutter contre les manipulations de l'information.

*

Ce bref état des lieux de la régulation internationale en matière de lutte contre les manipulations de l'information révèle une forte fragmentation des initiatives portées par différents acteurs privés et publics, une difficulté fondamentale à établir un consensus international sur la définition même du phénomène que les États cherchent à combattre et de sérieuses limites juridiques et politiques à sa mise en œuvre qui touche au cœur même des

valeurs démocratiques, de la liberté d'expression et du respect des droits de l'homme.

L'ABC proposé par Camille François offre un cadre utile pour démêler le phénomène et, plutôt que de chercher à en donner une définition exhaustive, distinguer les vecteurs pour en tirer des leviers d'action et de régulation. Ainsi, la lutte contre les acteurs malveillants peut-elle mobiliser les leviers du droit international, encore peu utilisés en la matière en raison des difficultés d'attribution et de qualification des opérations informationnelles. La lutte contre les comportements trompeurs, qui ciblent les modes de propagation illégitimes – voire illicites – des contenus plutôt que la nature des contenus eux-mêmes, concentre tous les efforts des plateformes, mais ne fait l'objet d'aucune régulation internationale.

Dans ces deux domaines, la marge de manœuvre des États est en pratique fortement contrainte par une asymétrie d'information et de réaction majeure entre les plateformes et les autres acteurs. Les plateformes se montrent extrêmement réticentes à donner cet accès à des chercheurs et des gouvernements en raison de leur culture, de leurs intérêts économiques, mais aussi des risques d'abus auxquels elles se sont trouvées confrontées et qui peuvent mettre en péril la confiance de leurs utilisateurs. À défaut, elles se trouvent en situation de mettre en œuvre des mesures, souvent hors de toute supervision démocratique. Pourtant, l'asymétrie relevée par Camille François ne saurait constituer, en droit, un obstacle à l'encadrement des pratiques des plateformes dans ces domaines, qui relève de la prérogative des États. La multiplicité des termes et définitions associées pour désigner le phénomène à combattre témoigne toutefois de la difficulté d'élaborer un consensus sur la définition de l'objet, liée d'une part à la complexité intrinsèque du sujet, mais aussi et surtout à sa dimension hautement politique en raison des risques d'atteinte aux droits humains en ligne.

La question est néanmoins au cœur des préoccupations des États dans les dialogues internationaux qui ont cours à l'ONU depuis l'automne 2019.

S’ils veulent éviter le piège qui s’ouvre devant eux, les États devront faire preuve de créativité et de rigueur pour définir des critères objectifs, qui prennent en compte les différentes dimensions du phénomène et ses défis propres. Ils peuvent s’appuyer utilement, mais pas exclusivement, sur le droit international. Les solutions ne peuvent pas faire l’économie d’une coopération avec le secteur privé, le monde académique et la société civile. L’enjeu est d’encadrer la lutte contre les pratiques de manipulation de l’information pour protéger les démocraties, sans en renier les valeurs fondamentales.

Pour aller plus loin

BENKLER Yochai, FARIS Robert, ROBERTS Hal, *Network Propaganda, Manipulation, Disinformation and Radicalization in American Politics*, Oxford, Oxford University Press, 2018.

CHASE Peter H., « The EU code of practice on disinformation : The difficulty of regulating a nebulous problem », Working Paper of the Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression, 29 août 2019.

DELERUE François, *Cyber Operations and International Law*, Cambridge, Cambridge University Press, 2020.

FRANÇOIS Camille, « Actors, behaviors, content : A disinformation ABC. Highlighting three vectors of viral deception to guide industry & regulatory responses », Working Paper of the Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression, 20 septembre 2019.

TANDOC Jr. Edson C. (éd.), « Defining “fake news” », *Digital Journalism*, 2018, vol. 6, n° 2, p. 137-153.

TSAGOURIAS Nicholas, « Electoral cyber interference, self-determination and the principle of non-intervention in cyberspace », EJIL : Talk !, 26 août 2019.

WARDLE Claire, DERAKHSAN Hossein, *Information Disorder : Toward an Interdisciplinary Framework for Research and Policy Making*, Council of Europe Report, 2017, DGI(2017)09, 107 p.

Glossaire

Amplification : mécanisme de diffusion massive d'informations par le biais de différents moyens, dont les bots et les trolls.

Attribution : fait d'imputer une cyberattaque à un attaquant identifié, en y apportant ou non des éléments de preuve. La preuve irréfutable d'une attaque étant en général difficile à apporter, certains États, comme la France, préfèrent ne pas désigner publiquement les agresseurs.

Big Data (ou **données massives** suivant la terminologie officielle française) : énormes volumes de données. La possession de ces banques de données massives et variées est devenue un objet de convoitise pour les États comme pour les acteurs privés. Leur contrôle peut être considéré comme un facteur de puissance.

Bot (diminutif de robot) : acteur automatisé ou semi-automatisé qui, par le biais de faux comptes sur les réseaux sociaux, amplifie artificiellement la diffusion d'informations. Les bots peuvent simuler des usagers de réseaux sociaux en donnant des notes positives, comme les likes et les retweets ; ils peuvent également animer des comptes en diffusant ou rediffusant du contenu.

Botnet (robot network, ensemble de robots) : ordinateurs ou appareils connectés détournés de leur usage légitime par l'attaquant. Ces automates existent en dehors des réseaux sociaux pour mener, par exemple, des attaques informatiques massives.

Bulles de filtre : offres personnalisées qui confortent les individus connectés dans leur point de vue. Ce mécanisme est susceptible de créer un déterminisme de l'information dans la mesure où l'historique de navigation d'un utilisateur donné agit comme un filtre pour limiter son accès à toute nouvelle information.

Chambres d'écho : affichage d'une sélection homogène de points de vue au sein d'une communauté.

Chatbots : programmes informatiques, pilotés par intelligence artificielle, dont le rôle est de simuler des conversations.

Ciblage : action de cibler certains groupes au moyen des outils numériques. Dans le domaine militaire, le ciblage peut être de deux natures, soit à large spectre afin d'influencer des populations, soit plus restreint en visant des individus (le terme consacré dans ce cas est *key leader engagement*). Dans le domaine civil, le ciblage informationnel s'inspire des stratégies marketing et publicitaires pour segmenter finement les publics visés et adapter les messages en conséquence.

Communication stratégique (STRATCOM) : utilisation coordonnée de différents outils de communication dans le but de produire un effet stratégique ou de mettre en œuvre une stratégie. La communication stratégique associe la diplomatie publique à la communication militaire opérationnelle pour appuyer la politique, les opérations et les actions d'une force armée.

Cyberespace : ensemble de réseaux reliés les uns aux autres par une série de connexions physiques et de protocoles de routage acheminant des paquets de données numériques qui, une fois mis bout à bout, forment un message (texte, image, vidéo, etc.). Le cyberespace est composé de différents réseaux, dont le principal est Internet.

Déception (anglicisme passé dans le langage militaire) : action militaire qui consiste à influencer les sources d'opposition dans leurs prises de décision, en les incitant à réagir de façon préjudiciable à leurs propres

intérêts. Elle utilise la ruse, la simulation et la dissimulation pour favoriser, à moindre coût, l'atteinte des objectifs.

Désinformation : processus de fabrication et de diffusion intentionnelle de fausses nouvelles. L'objectif recherché consiste à créer une fausse réalité suffisamment convaincante pour induire en erreur une audience cible.

Diplomatie publique : activités menées par des services d'information gouvernementaux ou privés pour s'adresser directement à des populations étrangères ou à des segments bien précis de celles-ci. La diplomatie publique comporte quatre types d'activités : la promotion de la politique étrangère ; la diplomatie culturelle officielle ; les échanges de personnes dans le cadre de programmes gouvernementaux ; les médias internationaux financés en totalité ou en partie par des fonds publics.

Espace informationnel : concept utilisé, surtout en Russie, pour qualifier le cyberespace. Il désigne un terrain de conflictualité virtuel, au même titre que des espaces géographiques réels, sur terre, sur mer, dans les airs et dans l'espace.

Fake news (ou **infox** suivant la terminologie officielle française) : informations ou discours intentionnellement faux ou distordus qui sont construits et diffusés à des fins de manipulation, en cherchant le plus souvent à contredire un discours dominant.

Guerre psychologique : terme générique désignant l'action militaire visant à utiliser ou à modifier les perceptions de l'adversaire ou d'une population afin d'obtenir, par un moyen non cinétique, une détérioration du moral ou de l'envie de combattre.

Influence militaire : action interarmées destinée à agir sur l'environnement humain des opérations. L'influence militaire vise à obtenir que les acteurs ciblés, qu'ils soient favorables, neutres ou hostiles, adoptent un comportement prédéfini qui serve les objectifs opérationnels.

Infox : voir **fake news**.

Internet : réseau à échelle mondiale, obtenu en reliant entre eux des réseaux à plus petite échelle. Véritables « briques élémentaires », les sous-réseaux qui composent Internet sont appelés systèmes autonomes.

Mème : idée ou concept simple, propagé de manière récurrente et virale à travers Internet, souvent sous la forme d'un visuel ou d'une image animée (GIF) issu de la culture médiatique.

Opération psychologique : opération planifiée en temps de paix, de crise ou de guerre et dirigée sur des publics ennemis, amis et neutres pour influencer leurs attitudes et leur comportement de manière à affecter la réalisation des objectifs politiques et militaires.

Psy-ops : terme doctrinal américain désignant les opérations psychologiques au niveau opérationnel et tactique. Les *psy-ops* associent des « capacités d'information » (*information-related capabilities*, **IRC**) et les opérations d'influence pour perturber la prise de décision des adversaires, tout en protégeant son processus décisionnel.

Résilience : capacité pour un système à continuer de fonctionner malgré une atteinte et à retourner à son état initial de fonctionnement. En ce sens, la résilience se distingue de la résistance qui est la capacité à subir des attaques sans dommages. Ce concept, relativement récent, a été emprunté à la psychologie. Il est utilisé pour comprendre comment des sociétés et des individus réagissent face à des agressions informationnelles.

Soft power : concept défini par le politologue américain Joseph Nye pour désigner la capacité d'attraction d'un État et celle de convaincre par la persuasion et la séduction plutôt que par la coercition.

Troll : acteur, généralement de mauvaise foi, qui peut s'attacher à titiller, à agacer, à humilier, à insulter, voire à harceler une personne ou une organisation. Ses motivations peuvent aller de la moquerie aux opérations de guerre psychologique en passant par le lobbying commercial.

Web 2.0 : terme forgé par Darcy DiNucci pour désigner les nouvelles caractéristiques de l'Internet qui reposent sur la mise en relation et

l’interaction horizontale des utilisateurs. Le Web originel laisse place au Web 2.0 à partir de la création des plateformes numériques d’échanges et des médias sociaux. La principale caractéristique du Web 2.0 est l’abolition de la barrière entre producteurs et consommateurs d’informations.

Bibliographie sélective

Ouvrages

ALLEN John, *Topologies of Power : Beyond Territory and Networks*, Londres, Routledge, 2016.

AUERBACH J., CASTRONOVO R., *The Oxford Handbook to Propaganda Studies*, Oxford, Oxford University Press, 2013.

ARDIS John A. S., KEENE Shima D., *Maintaining Information Dominance in Complex Environments*, Carlisle Barracks, United States Army War College Press, 2018.

BADOUARD Romain, *Le Désenchantement de l'Internet. Désinformation, rumeur et propagande*, Limoges, FYP Éditions, 2017.

BENKLER Yochai, FARIS Robert, ROBERTS Hal, *Network Propaganda, Manipulation, Disinformation and Radicalization in American Politics*, Oxford, Oxford University Press, 2018.

BJOLA Corneliu, HOLMES Marcus (dir.), *Digital Diplomacy : Theory and Practice*, Abingdon, Routledge, 2015.

CAGÉ Julia, HERVÉ Nicolas, VIAUD Marie-Luce, *L'Information à tout prix*, Paris, Institut national de l'audiovisuel, 2017.

CARDON Dominique, *Culture numérique*, Paris, Presses de Sciences Po, 2019.

COLON David, *Propagande. La manipulation de masse dans le monde contemporain*, Paris, Belin, 2019.

CULL Nicholas J., *Public Diplomacy : Foundations for Global Engagement in the Digital Age*, Cambridge, Polity, 2019.

DELERUE François, *Cyber Operations and International Law*, Cambridge, Cambridge University Press, 2020.

FLETCHER Tom, *Naked Diplomacy : Understanding Power and Statecraft in the Digital Age*, Londres, HarperCollins, 2016.

FRAU-MEIGS Divina, KINYINDU Alain, *Diversité culturelle à l'ère numérique. Glossaire critique*, Paris, La Documentation française, 2020.

FRAU-MEIGS Divina, *Faut-il avoir peur des fake news ?*, Paris, La Documentation française, 2020.

GAT Azar, *A History of Military Thought : From the Enlightenment to the Cold War*, Oxford, Oxford University Press, 2001.

HARBULOT Christian, *Les Fabricants d'intox. La guerre mondialisée des propagandes*, Paris, Lemieux, 2016.

HUYGHE François-Bernard, *Fake news : la grande peur*, Versailles, VA Press, 2018.

HUYGHE François-Bernard, KEMPF Olivier, MAZZUCCHI Nicolas, *Gagner les cyberconflits*, Paris, Economica, 2015.

LIMONIER Kevin, *Ru.net : géopolitique du cyberespace russophone*, Paris, L'Inventaire, « Les Carnets de l'Observatoire franco-russe », 2018.

MAURER Tim, *Cyber Mercenaries : The State, Hackers, and Power*, Cambridge/New York, Cambridge University Press, 2018.

MOWLANA Hamid, *Triumph of the Image : The Media's War in the Persian Gulf, a Global Perspective*, New York, Routledge, 2018.

MUZAMMIL M. Hussain, *State Power 2.0., Authoritarian Entrenchment and Political Engagement Worldwide*, Londres, Routledge, 2016, 1re éd.

NELSON Michael, *War of the Black Heavens : The Battles of Western Broadcasting in the Cold War*, Syracuse, Syracuse University Press, 1997.

PAMMENT James, *British Public Diplomacy and Soft Power : Diplomatic Influence and the Digital Revolution*, Londres, Palgrave, 2016.

POMERANTSEV Peter, WEIS Michael, *The Menace of Unreality : How the Kremlin Weaponizes Information, Culture and Money*, New York, Institute of Modern Russia, 2014.

POMERANTSEV Peter, *This Is Not Propaganda : Adventures in the War Against Reality*, Londres, Faber & Faber, 2019.

QUESSARD Maud, *Stratégies d'influence et guerres de l'information. Propagande et diplomatie publique des États-Unis depuis la guerre froide*, Rennes, PUR, 2019.

SEIB Philip, *Real-Time Diplomacy : Politics and Power in the Social Media Era*, New York, Palgrave, 2012.

SNOW Nancy, *Information War : American Propaganda, Free Speech and Opinion Control Since 9-11*, New York, Seven Stories Press, 2011.

STENGEL Richard, *Information Wars. How We Lost the Global Battle Against Disinformation and What Can We Do About It*, New York,

Grove Press, 2019.

SUROWIEC Pawel, MANOR Ilan (dir.), *Public Diplomacy and the Politics of Uncertainty*, New York, Palgrave, 2020.

TAILLAT Stéphane, CATTARUZZA Amaël et DANET Didier (dir.), *La Cyberdéfense. Politique de l'espace numérique*, Paris, Armand Colin, 2018.

TAYLOR Philip M., *Munitions of the Mind : A History of Propaganda*, Manchester, Manchester University Press, 2003, 3e éd.

Articles scientifiques

AUDINET Maxime, « Comment RT et Sputnik tissent la toile de Moscou à l'étranger », *La Revue des médias*, 19 juin 2019.

BERGÉ Jean-Sylvestre, GRUMBACH Stéphane, « La sphère des données : objet du droit international et européen », *Journal du droit international* (*Clunet*), 2016.

BLOUT Emily, « Iran's soft war with the West : History, myth, and nationalism in the new communications age », *SAIS Review of International Affairs*, 2015, vol. 35, no 2, p. 33-44.

CULL Nicholas J., « The long road to public diplomacy 2.0 : The Internet in US public diplomacy », *International Studies Review*, mars 2013, vol. 15, no 1, p. 123-139.

DOUZET Frédérick, « Le cyberespace, troisième front de la lutte contre Daesh », *Hérodote*, 2016, no 160, p. 223-238.

DOUZET Frédérick, DESFORGES Alix, « Du cyberespace à la datasphère. Le nouveau front pionnier de la géographie », *Netcom*, 2018, no 32-1/2, p. 87-108.

DUNCOMBE Constance, « Twitter and transformative diplomacy : Social media and Iran-US relations », *International Affairs*, 2017, vol. 93, n° 3, p. 545-562.

ERMOSHINA Ksenia, MUSIANI Francesca, « Migrating servers, elusive users : Reconfigurations of the Russian Internet in the post-Snowden era », *Media and Communication*, 22 mars 2017, vol. 5, n° 1, p. 42.

KARGAR Simin, RAUCHFLEISCH Adrian, « State-aligned trolling in Iran and the double-edged affordances of Instagram », *New Media & Society*, 2019, vol. 21, n° 7, p. 1506-1527.

KEMPF Olivier, MAZZUCCHI Nicolas, « Cyberespace et intelligence économique », *Géoéconomie*, novembre-décembre 2015, n° 77, p. 45-62.

LIMONIER Kevin, GÉRARD Colin, « Guerre hybride russe dans le cyberespace », *Hérodote*, 2017, n° 166-167, p. 152-153.

MAZZUCCHI Nicolas, « L'économie, cible privilégiée de la guerre informationnelle ? », *Revue Défense nationale*, mai 2014, n° 770, p. 22-27.

MUIR James A., VAN OORSCHOT Paul C., « Internet geolocation : Evasion and counterevasion », *ACM Comput. Surv.*, décembre 2009, vol. 42, n° 1, p. 4-23.

NIMMO Ben, « Measuring traffic manipulation on Twitter », *Oxford Internet Institute*, janvier 2019.

NYE Joseph, « Protecting democracy in an era of cyber information war », *Hoover Institution*, novembre 2018, n° 318.

PAHLAVI Pierre, « Understanding Iran's media diplomacy », *Israel Journal of Foreign Affairs*, 2012, vol. VI, n° 2, p. 21-33.

SUROWIEC Pawel, LONG Philip, « Hybridity and soft power statecraft : The "GREAT" campaign », *Diplomacy and Statecraft*, 2020, vol.

31/1, p. 168-195.

Revues et numéros spéciaux

FOREIGN AFFAIRS, « World War Web. The fight for Internet's future », septembre-octobre 2018, vol. 97, n° 5.

HÉRODOTE, « Géopolitique de la datasphère », mai-juin 2020, n° 177-178.

POLITICS, numéro spécial « The soft power of hard states », 2015, vol. 35, n° 3-4, p. 213-377.

QUESTIONS INTERNATIONALES, « Révolutions technologiques : d'un monde à l'autre », Paris, La Documentation française, mai-août 2018, n° 91-92.

Rapports

CLÜVER ASHBROOK Cathryn, *From Digital Diplomacy to Data Diplomacy. International Politics and Society*, 14 janvier 2020.

COMMISSION EUROPÉENNE, *Plan d'action contre la désinformation*, JOIN/2018/36 final.

DARCZEWSKA Jolanta, « The anatomy of Russian information warfare. The Crimean operation, a case study », *Point of View*, Varsovie, Centre for Eastern Studies, mai 2014, n° 42.

FRANÇOIS Camille, « Actors, behaviors, content : A disinformation ABC. Highlighting three vectors of viral deception to guide industry & regulatory responses », Working Paper of the Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression, 20 septembre 2019.

FRANÇOIS Camille, NIMMO Ben, *The IRACopyPasta Campaign, Russian Accounts Posing as Americans on Instagram Targeted Bothsides of Polarizing Issues Ahead of the 2020 Election*, New York, Graphika, octobre 2019.

FRIED Daniel, POLYAKOVA Alina, *Democratic Defense Against Disinformation*, Washington, Atlantic Council, février 2018.

HÉMEZ Rémy, *Opérations de déception. Repenser la ruse au XXIe siècle*, Paris, IFRI, 2018.

JEANGÈNE VILMER Jean-Baptiste, *The « Macron Leaks » Operation : A Post-Mortem*, Atlantic Council & IRSEM Report, 2019.

JEANGÈNE VILMER Jean-Baptiste, ESCORCIA Alexandre, GUILLAUME Marine, HERRERA Janaina, *Les Manipulations de l'information : un défi pour nos démocraties*, rapport conjoint du CAPS (Centre d'analyse, de prévision et de stratégie du ministère de l'Europe et des Affaires étrangères) et de l'IRSEM (Institut de recherche stratégique de l'École militaire du ministère des Armées), 2018.

KAVANAUGH Jennifer, RICH Michael D., *Truth Decay : An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life*, Santa Monica, RAND Corporation, 2018.

LIMONIER Kevin, « Diffusion de l'information russe en Afrique. Essai de cartographie générale », IRSEM, 13 novembre 2018, Note de recherche n° 66, 21 p.

MANSTED Katherine, ROSENBACH Eric, *The Geopolitics of Information*, Cambridge, Belfer Center, Harvard Kennedy School of Government, mai 2019.

MARANGÉ Céline, *Les stratégies et les pratiques d'influence de la Russie*, IRSEM, mars 2017, *Études*, n° 49, 55 p.

MEAE, « Technologies et puissance », *Les Carnets du CAPS*, Paris, automne 2018, n° 26.

NOCETTI Julien, « Guerres de l'information : le Web russe dans le conflit en Ukraine », Institut français de relations internationales, septembre 2015, Focus stratégique n° 62.

PAUL Christopher, CLARKE Colin P., SCHWILLE Michael, HLÁVKA Jakub P., BROWN Michael A., DAVENPORT Steven S., PORCHE III Isaac R., HARDING Joel, *Lessons From Others for Future U.S. Army Operations In and Through the Information Environment*, Santa Monica, RAND Corporation, 2018.

RACZ Andras, *Russia's Hybrid War in Ukraine. Breaking the Enemy's Ability to Resist*, Helsinki, The Finnish Institute of International Affairs, 2015, FIIA Report, n° 43.

TOUCAS Boris, *The Macron Leaks : The Defeat of Informational Warfare*, Center for Strategic and International Studies, 2017.

WARDLE Claire, DERAKHSAN Hossein, *Information Disorder : Toward an interdisciplinary framework for Research and Policy Making*, Council of Europe Report, 2017, DGI (2017)09.

Les auteurs

Maxime Audinet est chercheur à l'IRSEM et docteur de l'université Paris Nanterre. Il était auparavant chercheur au centre Russie/NEI de l'Institut français des relations internationales (IFRI). Ses recherches portent sur la politique d'influence russe à l'ère post-soviétique. Elles se concentrent sur l'interprétation du concept de *soft power* en Russie (*mâgkaâ sila*), ainsi que sur les acteurs et les pratiques de sa diplomatie publique (diplomatie culturelle, médias internationaux). Il a enseigné à l'université Paris Nanterre et à Sciences Po Paris. Parmi ses publications, on compte « Diplomaties publiques concurrentielles dans la crise ukrainienne. Le cas de RT et Ukraine Today », *Revue d'études comparatives Est-Ouest*, 2018, vol. 2, n° 2, p. 171-204, et « La stratégie d'influence informationnelle et numérique de la Russie en Europe », *Hérodote*, 2017, n° 164, p. 123-144 (avec Kevin Limonier).

Pascal Brangetto est commissaire des armées et diplômé de l'IEP de Paris et de l'université Paris 1 – Panthéon-Sorbonne. Ayant servi successivement au sein de formations de l'armée de terre, il a été déployé en Afghanistan en 2010. De 2013 à 2016, il a été affecté en qualité de conseiller juridique opérationnel au centre d'excellence de cyberdéfense à Tallinn (Estonie). À cette occasion, il a participé aux travaux du centre, notamment dans le domaine de l'applicabilité du droit international au cyberespace. Il travaille actuellement au profit du commandement du

service militaire adapté au sein du ministère des Outre-mer chargé des questions budgétaires.

Paul Charon est directeur du domaine « Renseignement, anticipation et menaces hybrides » de l'Institut de recherche stratégique de l'École militaire (IRSEM). Docteur en études politiques de l'École des hautes études en sciences sociales (EHESS), titulaire d'un MBA (HEC), il est également diplômé en langue et civilisation chinoises (université Paris-Diderot et Beijing Language and Culture University, BLCU) et en droit (université Panthéon-Assas). Avant de rejoindre l'IRSEM, il a travaillé plus de dix ans en qualité d'analyste du renseignement, puis de conseiller prospective, au sein du ministère des Armées. Il a également été chercheur associé de l'antenne franco-chinoise en sciences humaines et sociales de l'université Qinghua à Pékin. Ses travaux portent sur la Chine (opérations d'influence, services de renseignement) et les méthodes d'analyse du renseignement et d'anticipation des surprises stratégiques. Il enseigne à Sciences Po Paris, Sciences Po Saint-Germain-en-Laye, l'université Paris 2 – Panthéon-Assas, ainsi qu'à l'université Rey Juan Carlos de Madrid.

Nicholas John Cull est professeur de diplomatie publique à l'université de Californie du Sud (USC) où il dépend à la fois du Centre de communication sur le leadership (CCL) et du Centre sur la diplomatie publique (CPD). Il est l'un des plus prolixes auteurs d'études sur la diplomatie publique. Parmi ses travaux récents : *Public Diplomacy : Foundations for Global Engagement in the Digital Age* (Polity, 2019) et, avec Nancy Snow, *The Routledge Handbook of Public Diplomacy* (Routledge, 2020, 2e éd.). Ses premiers travaux ont été consacrés au développement de la diplomatie publique aux États-Unis. Originaire du Royaume-Uni, il a travaillé avec le British Council et le Foreign Office ; en 2019, il était professeur invité à l'université d'Oxford ; il est membre du Conseil sur la diplomatie publique.

Fatiha Dazi-Héni est chercheuse en science politique, spécialiste des monarchies de la péninsule Arabique et du golfe Persique, à l'Institut de recherche stratégique de l'École militaire (IRSEM). Docteure en science politique (Institut d'études politiques de Paris), elle a enseigné à Sciences Po Lille et à l'université Paris 1 – Panthéon-Sorbonne et assure la direction pédagogique de la formation continue de Sciences Po Paris « Investir et négocier au Moyen-Orient ». Avant de rejoindre l'IRSEM, elle était conseiller auprès de la Direction des affaires stratégiques du ministère de la Défense. Elle mène des recherches sur le Conseil de coopération du Golfe, les évolutions sociales et politiques de la péninsule Arabique et les enjeux sécuritaires et stratégiques au Moyen-Orient. Elle est l'auteur de *Monarchies et sociétés d'Arabie. Le temps des confrontations* (Paris, Presses de Sciences Po, 2006) et de *L'Arabie en 100 questions* (Paris, Tallandier, 2017 et 2018).

François Delerue est docteur en droit et chercheur en cyberdéfense et droit international à l'Institut de recherche stratégique de l'École militaire (IRSEM). Il est également rapporteur pour le droit international de l'Academic Advisory Board du projet EU Cyber Direct et enseignant à Sciences Po. Il mène des recherches sur les questions de cyberdéfense et de cybersécurité sous l'angle juridique, stratégique et politique. Il s'intéresse tout particulièrement au droit international, aux normes et à la coopération internationale, ainsi qu'aux différents types d'acteurs impliqués (États, entreprises privées, organisations non gouvernementales, etc.). Plus généralement il s'intéresse à l'impact des nouvelles technologies (conquête spatiale, robotique, intelligence artificielle, etc.) sur le droit international et les relations internationales. Son ouvrage *Cyber Operations and International Law* est paru chez Cambridge University Press (Cambridge Studies in International and Comparative Law) en mars 2020.

Frédérick Douzet est professeure des universités en géopolitique à l'Institut français de géopolitique de l'université Paris 8 et directrice du projet Géopolitique de la datasphère (GEODE). Ses recherches portent sur les enjeux stratégiques et géopolitiques de la révolution numérique. Elle est membre de la Global Commission on the Stability of Cyberspace depuis février 2017 et du comité d'éthique de la Défense depuis janvier 2020. En 2017, elle a participé au comité de rédaction de la *Revue stratégique de défense et de sécurité nationale*. De 2013 à 2018, elle a dirigé la chaire Castex de cyberstratégie de l'Institut des hautes études de Défense nationale (IHEDN). Frédérick Douzet a été nommée membre junior de l'Institut universitaire de France en 2006 et a reçu plusieurs prix pour ses recherches. Elle a coordonné le numéro 177-178 de la revue *Hérodote* « Géopolitique de la datasphère » (2020).

Amélie Férey est chercheuse postdoctorale en science politique à l'IRSEM et au Centre de recherches internationales de Sciences Po (CERI). Ses publications traitent des thèmes suivants : l'éthique et le droit de la guerre, le contre-terrorisme, le libéralisme politique, le conflit israélo-palestinien et ses représentations. Son livre *Les Assassinats ciblés. Critique du libéralisme armé*, issu de sa thèse, va paraître aux éditions du CNRS. Ses recherches actuelles portent sur le *lawfare* et les guerres « douces » (*soft wars*) dans le contexte israélo-palestinien. Docteure en science politique (IEP de Paris), elle est enseignante à Sciences Po Paris, à l'université Paris 2 – Panthéon-Assas et à l'université Lyon 3. Elle a également été chercheuse invitée au Centre français de recherche (CNRS/MAE) à Jérusalem.

Divina Frau-Meigs est professeur à l'université Sorbonne-Nouvelle et titulaire de la chaire UNESCO « Savoir-devenir à l'ère du développement numérique durable : maîtriser les cultures de l'information ». Boursière Fulbright et Lavoisier, elle est diplômée de l'université de la Sorbonne, de

l'université de Stanford (Palo Alto) et de l'Annenberg School for Communications de l'université de Pennsylvanie à Philadelphie. Sociologue des médias, elle est spécialiste des questions de réception et d'usage des technologies de l'information et de la communication. À ce titre, au niveau européen, elle fait partie de deux groupes d'experts de haut niveau de l'Union européenne, l'un sur la désinformation et l'autre sur l'éducation aux médias. Elle est l'auteur de nombreux articles dans des revues nationales et internationales et d'une trentaine d'ouvrages en plusieurs langues, dont *Faut-il avoir peur des « fake news » ?* (La Documentation française, 2019) et *The Handbook on Media Education Research* (Wiley, 2020).

Rémi Géraud-Stewart est chercheur au sein du Groupe de sécurité de l'information du département d'informatique de l'École normale supérieure de Paris, chercheur associé à la chaire Castex de cyberstratégie (IHEDN) et chercheur associé au groupe Géopolitique de la datasphère (GEODE, Paris 8), et responsable de cours à Centrale Supélec (cybersécurité, cryptographie). Ses travaux portent sur les outils mathématiques liés à l'exploitation des réseaux, réseaux sociaux, et systèmes d'information. Parmi ses publications liées au sujet du livre, on compte : Frédérick Douzet, Kevin Limonier, Jérémy Robine, Kavé Salamatian, Rémi Géraud et Romain Campigotto, « Les nouveaux territoires stratégiques du cyberespace : le cas de la Russie », *Stratégique*, 2017/4, n° 117, p. 169-186 ; Rémi Géraud, « Cyberspace and time : A light through the fog ? », *CIST2018 – Représenter les territoires/Representing territories*, Rouen, CIST, mars 2018.

Aude Géry est post-doctorante au sein de GEODE, centre de recherche et de formation sur la politique de la datasphère de l'université Paris 8. Sa thèse porte sur la lutte contre la prolifération des armes numériques en droit international. Ses recherches portent plus généralement sur le droit

international des technologies de l'information et de la communication dans le contexte de la sécurité internationale, sous un angle à la fois juridique et géopolitique. Elle travaille ainsi sur les stratégies juridiques des États, les négociations internationales en cours et la coopération internationale.

Éric Gomez est officier supérieur dans l'armée de l'air et chef de corps du Centre national de ciblage, un organisme à vocation interarmées fortement en prise avec les opérations. Chercheur associé à l'Institut de recherche stratégique de l'École militaire (IRSEM), chercheur affilié et expert associé au Service historique de la défense (SHD), il réalise une thèse au sujet de la conduite du changement dans la communauté française du renseignement au sein de l'Institut de recherche Montesquieu (IRM) de l'université Bordeaux-Montaigne. Ses recherches portent sur l'histoire du renseignement français et son organisation. Diplômé du master de gestion publique de l'université Paris-Dauphine et de l'École nationale d'administration (ENA), il occupe la fonction de délégué de la section défense de l'Association des anciens élèves de l'ENA (AAEENA).

Jean-Baptiste Jeangène Vilmer est directeur de l'Institut de recherche stratégique de l'École militaire (IRSEM, ministère des Armées) et *nonresident Senior Fellow* à l'Atlantic Council (Washington DC). Auditeur de l'IHEDN, membre du conseil scientifique du Collège de défense de l'OTAN, il enseigne également à la Paris School of International Affairs (PSIA) de Sciences Po. Docteur en science politique et en philosophie, juriste, il était précédemment en poste au ministère des Affaires étrangères, à la faculté de droit de McGill University et au département de War Studies du King's College London. Auteur de 20 livres, ses recherches portent sur les relations internationales et les conflits armés. Sur les menaces hybrides et les manipulations de l'information, il a notamment publié deux rapports : *Les Manipulations de l'information* (CAPS/IRSEM, 2018) et *The « Macron Leaks » Operation : A Post-Mortem* (IRSEM/Atlantic Council, 2019).

Kevin Limonier est maître de conférences en études slaves à l'Institut français de géopolitique (université Paris 8). Il est également directeur adjoint du centre GEODE (www.geode.science) et directeur scientifique de l'Observatoire de l'infosphère russophone, une structure de recherche dédiée à l'analyse des espaces numériques post-soviétiques. Il intervient dans plusieurs formations sur les questions cybernétiques, notamment à Saint-Cyr-Coëtquidan, et fut pendant plusieurs années enseignant à l'université d'État des sciences humaines de Russie (RGGU, Moscou). Ses recherches portent sur le développement de nouvelles méthodes de cartographie du cyberespace, notamment dans le contexte post-soviétique. Il est plus largement spécialiste de l'Internet russophone (*Ru.net : géopolitique du cyberespace russophone*, Paris, L'Inventaire, « Les Carnets de l'Observatoire franco-russe », 2018) et des politiques territoriales d'innovation en URSS et dans la Russie contemporaine (*L'Archipel des savants : histoire des anciennes villes d'élite du complexe scientifique soviétique*, Paris, B2, 2017).

Céline Marangé est chercheuse au sein de la Division Recherches, Études et Enseignement (DREE) du Service historique de la Défense (SHD), consultante permanente du Centre d'analyse, de prévision et de stratégie (CAPS) et chercheuse associée au Centre de recherche en histoire des Slaves de l'université Paris 1 - Panthéon-Sorbonne. Docteure en science politique (Institut d'études politiques de Paris) et spécialiste des relations internationales, elle mène des recherches sur la politique étrangère russe et les enjeux de sécurité en Europe. Elle a enseigné à Columbia, à Harvard, à l'INALCO et à Sciences Po, et a été *Fox International Fellow* à l'université de Yale, puis post-doctorante à l'université Paris 1. De 2014 à 2020, elle a été chercheuse sur la Russie et l'Ukraine à l'Institut de recherche stratégique de l'École militaire (IRSEM). Elle a notamment publié *Les Stratégies et les Pratiques d'influence de la Russie* (IRSEM, 2017, Étude

n° 49) et cosigné avec Nicolas Mazzucchi « Contrôle du cyberespace et souveraineté numérique en Russie » (*Les Cahiers français*, 2020, n° 415).

Nicolas Mazzucchi est chargé de recherche à la Fondation pour la recherche stratégique (FRS) où il est en charge des domaines énergie, cyber et matières premières. Docteur en géographie économique, qualifié aux fonctions de maître de conférences, il enseigne depuis plus d'une dizaine d'années au sein de l'enseignement supérieur militaire (École de guerre, CHEM, EMSST), à Sciences Po Paris ainsi que dans d'autres institutions. Auditeur de la 25e promotion de l'École de guerre, officier de réserve de la Marine nationale, conseiller scientifique de Futuribles International et membre du groupe « sécurité » du Hub France IA, il a conduit une carrière de chercheur et d'opérationnel dans le privé et au sein du ministère des Armées. Nicolas Mazzucchi est co-auteur avec François-Bernard Huyghe et Olivier Kempf de *Gagner les cyberconflits* (Economica, 2015) et auteur d'*Énergie, ressources, technologies et enjeux de pouvoir* (Armand Colin, 2017).

Ben Nimmo est directeur de recherche chez Graphika, une société d'analyse des réseaux sociaux établie à New York. Son domaine d'expertise est l'étude des opérations d'information à grande échelle menées par des acteurs non gouvernementaux utilisant les plateformes Internet. Ses premiers travaux se sont concentrés sur la Russie et les méthodes pour anticiper les campagnes de désinformation en utilisant le modèle des 4D, puis ses analyses ont porté sur les tentatives d'influence de l'Iran, la Chine, l'Arabie saoudite, l'extrême droite transnationale, et les groupes communautaires. Parmi ses publications récentes : avec Camille François, *The IraCopyPasta Campaign, Russian Accounts Posing as Americans on Instagram Targeted Bothsides of Polarizing Issues Ahead of the 2020 Election* (New York, Graphika, octobre 2019).

Valérie Niquet est spécialiste des relations internationales et des questions stratégiques en Asie et responsable du pôle Asie à la Fondation pour la recherche stratégique (FRS). Elle est l'auteur de nombreux articles et études consacrés à l'évolution des équilibres régionaux et aux questions stratégiques en Asie, aux politiques de défense des grandes puissances régionales et à l'évolution des systèmes politiques chinois et japonais. Valérie Niquet est conseiller du Centre d'analyse, de prévision et de stratégie (CAPS). Elle intervient régulièrement dans les débats stratégiques consacrés à l'Asie. Elle est l'auteur de la première traduction directe du chinois en français de *L'Art de la guerre* de Sun Zi. Ses deux derniers ouvrages, *La Puissance chinoise. Un géant fragile ?* et *Le Japon. Un modèle en déclin ?*, ont été publiés chez Tallandier, dans la collection « En 100 questions », en 2017 et en 2020.

Pierre Pahlavi, professeur titulaire au Collège des Forces canadiennes de Toronto (Ontario), est actuellement directeur du département de la sécurité et des affaires internationales et directeur adjoint du département des études de la défense. Ses principaux domaines d'expertise et ses publications portent sur les stratégies d'influence, la politique étrangère de l'Iran et les défis hybrides. Son dernier livre sur la révolution iranienne publié aux éditions Perrin en 2017 a reçu le prix Diane Potter-Boès décerné chaque année par l'Académie française pour le meilleur livre sur le Moyen-Orient. Il travaille ponctuellement à titre de consultant média sur la question iranienne et est un membre actif de l'Observatoire sur le Moyen-Orient et l'Afrique du Nord de la chaire Raoul-Dandurand, UQAM (Québec).

Benjamin Pajot est chargé de mission sur les enjeux numériques au sein du Centre d'analyse, de prévision et de stratégie (CAPS) du ministère de l'Europe et des Affaires étrangères. Ancien élève de l'École normale supérieure de Lyon en histoire contemporaine, il est également titulaire d'un master d'expertise des conflits armés de l'université Paris 1 – Panthéon-

Sorbonne. Ses recherches portent sur la géopolitique du numérique et des nouvelles technologies. Il s'est notamment intéressé aux rapports de force internationaux dans le domaine de l'intelligence artificielle (« La guerre de l'intelligence artificielle aura-t-elle lieu ? », *Les Carnets du CAPS*, 2018, n° 26) et à la rivalité technologique opposant la Chine aux États-Unis (« La rivalité sino-américaine, facteur structurant de la géopolitique du numérique », in *Enjeux internationaux des activités numériques*, Larcier, à paraître).

Marianne Péron-Doise est diplômée de l'IEP de Aix-en-Provence et titulaire d'un diplôme d'études approfondies d'histoire. Elle est chercheuse sur l'Asie du Nord (péninsule coréenne, Japon) et chargée du programme Sécurité maritime internationale à l'Institut de recherche stratégique de l'École militaire (IRSEM). Elle a été auparavant conseiller politique auprès du commandement maritime de l'OTAN à Northwood au Royaume-Uni (2012-2015) et chef du bureau Asie-Pacifique et Asie centrale à la Délégation aux Affaires stratégiques du ministère de la Défense (2008-2012). Parmi ses dernières publications : « Deterrence and dialogue : The US-South Korea alliance in search of a new lease of life in the face of Kim Jong-un's "nuclear diplomacy" », *in* Maud Quessard, Frédéric Heurtebize et Frédérick Gagnon (dir.), *Alliances and Power Politics in the Trump Era* (Palgrave Macmillan, 2020) et « La Défense japonaise : une posture opérationnelle et capacitaire en expansion », *in* Guibourg Delamotte (dir.), *Le Japon et le Monde* (CNRS Éditions, 2019).

Maud Quessard est directrice du domaine « Espace Euratlantique à l'IRSEM », maître de conférences en civilisation nord-américaine, diplômée de l'Institut d'Études politiques (IEP) de Bordeaux et spécialiste de politique étrangère américaine. Elle a enseigné à l'université de Poitiers, à l'IEP de Bordeaux, à Paris 2 Panthéon-Assas et à Sciences Po Paris. Ses recherches portent sur la diplomatie publique, le *soft power* américain, les

guerres de l’information et les stratégies d’influence. Elle a bénéficié du programme de soutien à la recherche de l’IHEDN, a été *visiting fellow* au département d’histoire de l’université de Harvard en 2015. Elle est l’auteur d’une monographie *Stratégies d’influence et guerres de l’information. Propagande et diplomatie publique des États-Unis depuis la guerre froide* (PUR, 2019).

TABLE DES MATIÈRES

Préface - Jean-Baptiste Jeangène Vilmer

Introduction - Le nouvel âge des guerres de l'information - Céline Marangé et Maud Quessard

L'arme de l'information comme héritage de la guerre froide

La propagande de guerre comme matrice initiale

La diplomatie publique et la guerre psychologique

Le rôle de la subversion dans la lutte idéologique

L'information comme enjeu de sécurité nationale

La sécuritisation de l'information

Les préventions des régimes autoritaires

Les vulnérabilités des régimes démocratiques

La révolution numérique comme rupture stratégique

Un nouvel espace-temps sur le théâtre d'opérations

Une saturation de l'espace informationnel

La fin de la suprématie technologique américaine

Pour une approche globale des guerres de l'information

I - Techniques et usages de l'information

Chapitre 1 - L'arme de l'information dans les conflits armés - Nicolas Mazzucchi

Invariants historiques et développement des médias

La désinformation, une pratique aussi ancienne que l'histoire

La manipulation dans les conflits du xxe siècle

L'enjeu du moral dans les conflits de la guerre froide

Le contrôle de l'information dans les conflits post-guerre froide

L'information au cœur des conflits contemporains

Le pouvoir égalisateur du cyberespace

Le conflit israélo-libanais de 2006 comme exemple

Des doctrines militaires intégrant les opérations d'information

Daech, cas d'école de l'organisation infocentrée

La lutte pour l'attention comme enjeu majeur des guerres de demain

Un cyberespace plus ample et plus intrusif

Des manipulations plus sophistiquées

La guerre de l'attention 3.0

Les enjeux militaires afférents

Focus 1 - Le ciblage dans le domaine militaire - Lieutenant-colonel Éric Gomez

Le ciblage au xxe siècle : de la frappe de masse à la « frappe chirurgicale »

Le ciblage large spectre : synchroniser les effets pour une efficacité accrue

Le ciblage dans les opérations spéciales et les opérations de renseignement

Chapitre 2 - Les couches basses du cyberespace : contrôle des flux et cartographie d'Internet - Kevin Limonier

Les attributs de la couche infrastructurelle

Les enjeux du contrôle des couches basses

Les « briques élémentaires » d'Internet

Le voyage d'un paquet de données

Déni d'accès, espionnage et contrôle de l'information

Les manipulations physiques du réseau

Les manipulations de routage

Focus 2 - La guerre électronique - Lieutenant-colonel Éric Gomez

Les débuts de la guerre électronique

Des ondes radio au cyberespace

La guerre électronique à l'ère numérique

Chapitre 3 - Les techniques d'amplification sur les réseaux sociaux - Ben Nimmo

L'amplification authentique et inauthentique

Les comptes automatisés (bots)

Les types de comptes amplificateurs

Percer parmi les tendances majeures

La manipulation experte : le cas de la France

Focus 3 - Les preuves de la manipulation de l'information - Rémi Géraud-Stewart

Reconnaître le faux

Reconnaître le vrai

Reconnaître l'influence par ses objectifs

La question de la « source »

II - Les guerres de l'information en contexte autoritaire

Chapitre 4 - La Russie : « l'espace informationnel » comme terrain de conflictualité - Maxime Audinet et Céline Marangé

Une vision défensive de l'information

L'information comme composante de la sécurité nationale

L'information comme vecteur de diplomatie publique

L'information comme terrain de rivalité mondiale

Un large spectre d'actions offensives

Le recours à des médias d'influence « alternatifs »

La manipulation de l'information à des fins de subversion politique

Le contrôle de l'information dans les opérations armées

Chapitre 5 - La Chine : une modernisation des pratiques de guerre de l'information - Valérie Niquet

Les fondements théoriques de la guerre de l'information en Chine

Ruse et stratagème : l'héritage classique

Manipulation et propagande : l'apport lénino-maoïste

Le contrôle de l'information à l'époque contemporaine : propagande et contre-propagande

Les organes du parti en charge de la propagande interne

Le rôle d'Internet : ouverture initiale et adaptation de la censure

Le rôle de la propagande extérieure dans la guerre de l'information

Des objectifs en évolution

Des instruments intégrés et diversifiés

La dimension militaire de la guerre de l'information

Renouvellement conceptuel et mise en œuvre des moyens

Retour aux sources : la guerre du peuple appliquée à la guerre de l'information

Focus 4 - Taïwan : laboratoire des manipulations de l'information chinoises - Paul Charon

La matrice doctrinale

Subvertir Taïwan

Vers une complexification des opérations chinoises

Chapitre 6 - Corée du Nord : la stratégie informationnelle de Kim Jong-un - Marianne Péron-Doise

Les ressorts informationnels d'une idéologie totalitaire

Les leviers techniques de l'autarcie informationnelle

L'information comme vecteur d'« ouverture »

L'information et le cyber comme outils de guerre

Chapitre 7 - L'Iran : stratégie asymétrique et diplomatie de masse - Pierre Pahlavi

L'arme informationnelle au cœur d'une stratégie globale

Une vision du monde placée sous le mode obsidional

De la dissymétrie à l'asymétrie : l'information comme arme stratégique

L'influence du Corps des Gardiens de la révolution islamique

Une diplomatie publique sophistiquée et hybride

L'IRIB comme chef d'orchestre

Les grands médias audiovisuels et leurs publics cibles

Nouveaux médias et réseaux privés

Chapitre 8 - Les monarchies du Golfe : les guerres de l'information dans la crise de juin 2017 - Fatiha Dazi-Héni

Les ressorts de la crise du 5 juin 2017

Les effets de la personnalisation des régimes néopatriarcaux du Golfe

La dynamique des réseaux sociaux dans l'environnement informationnel

Des narratifs nationalistes exacerbés au cœur de la crise

Abu Dhabi versus Qatar : des stratégies informationnelles aux antipodes

Al-Jazeera, le coup d'avance de la diplomatie publique du Qatar

L'affirmation de la diplomatie publique d'Abu Dhabi

Des stratégies d'influence opposées pour gagner le soutien des États-Unis

Le lobbying combatif d'Abu Dhabi

L'approche institutionnelle du Qatar

III - Les démocraties face aux guerres de l'information

Chapitre 9 - Le Royaume-Uni : appréhender une sécurité réputationnelle - Nicholas J. Cull

La Grande-Bretagne et les débuts de la guerre de l'information

La Grande-Bretagne et les audiences étrangères

L'avènement de la guerre numérique de l'information

La réponse britannique

L'affaire Skripal et ses suites

Appréhender une sécurité réputationnelle

Chapitre 10 - Les États-Unis : la militarisation de la diplomatie publique - Maud Quessard

Le virage numérique de la diplomatie publique de Bush à Obama

Des médias traditionnels aux réseaux sociaux

Information et « liberté d'Internet »

Le contrôle de l'information au cœur des enjeux de la diplomatie numérique

L'information comme vecteur d'influence militaire

Enjeux politiques et pratiques militaires

Le rôle fondamental des acteurs de terrain

Le manque de coordination des acteurs

Les réponses institutionnelles aux guerres cyber

Les vulnérabilités du géant militaire américain

L'affirmation d'une posture offensive

Chapitre 11 - Israël : de la hasbara à la guerre cognitive - Amélie Férey

La hasbara et la communication politique

Les racines historiques du concept

Entre propagande et diplomatie publique

Des acteurs institutionnels nombreux

Le développement de la « guerre cognitive »

De la guerre psychologique à la guerre cognitive

Le versant offensif : collecte de l'information et guerre cyber

Le versant défensif : l'amélioration de l'image de l'armée

Une combinaison d'approches contre l'Iran

Critique d'Israël ou faillite de la hasbara ?

Chapitre 12 - Le Japon : une prise de conscience récente des enjeux informationnels - Valérie Niquet

La puissance du soft power au Japon

Une diplomatie publique plus active

Des moyens renforcés

Les limites

Guerre de l'information et normes sur Internet

Chapitre 13 - La France : quelle stratégie de résilience face aux manipulations de l'information ? - Benjamin Pajot

L'information, terrain historique d'influences étrangères

La France et la guerre de l'information au xxe siècle

Les « Macron Leaks » ou l'entrée dans l'ère des manipulations de l'information

Une réponse étatique en deux volets

Le niveau régalien : vigilance renforcée à l'égard des menaces et coordination en cours

Le niveau législatif : une prévention des risques électoraux

Une co-construction de la résilience de la société française

Une sensibilisation croissante de la société

Initiatives partagées et multi-acteurs

IV - Les réponses scientifiques, juridiques et politiques

Chapitre 14 - Les enjeux de la réception : comment mesurer l'influence de la désinformation ? - Divina Frau-Meigs

Caractériser les mécanismes de la désinformation

La polarisation des publics et l'exposition sélective

La propagation locale des discours radicalisés

La systématisation des attaques

Analyser les vecteurs de diffusion des infox

L'influence pilotée par les algorithmes : chambres d'écho et bulles de filtre

L'influence pilotée par les humains : biais cognitifs et influence continue

La crise épistémique née de la défiance généralisée

Évaluer l'influence en désinformation

L'étude du rôle des usagers : vers un nouveau modèle de l'influence

Les limites de l'enquête

Chapitre 15 - Les menaces numériques en période électorale - François Delerue

Les élections présidentielles américaines : un foisonnement d'opérations diverses

Les élections françaises de 2017 : une meilleure anticipation

Les opérations cyber contre les processus électoraux

Les atteintes à la liberté de choix des électeurs

La panoplie des réponses possibles

Chapitre 16 - Panorama des mesures prises contre les manipulations de l'information - Jean-Baptiste Jeangène Vilmer

La mobilisation des États

Le design organisationnel

Le rôle des parlements

La sensibilisation de la population

La régulation des médias

La coopération internationale

Le partage du renseignement

Les formats multilatéraux : UE, OTAN, G7

Les think tanks, passeurs d'idées

L'implication de la société civile

Les limites des mesures prises

Focus 5 - L'OTAN et la guerre de l'information - Commissaire principal Pascal Brangetto

La doctrine cyber de l'OTAN

La défense collective dans le cyberespace

La protection des réseaux de l'OTAN

La préparation aux guerres de l'information

L'intégration du cyber dans les exercices de l'OTAN

Les exercices classiques

Les exercices proprement cyber

Les exercices de défi technique

Chapitre 17 - La régulation pour contrer les manipulations de l'information en ligne : l'impossible consensus international ? - Frédérick Douzet et Aude Géry

Neutraliser les acteurs malveillants

Un recours limité au droit international

L'engagement prudent des plateformes du Web

Cibler les comportements trompeurs

Le rôle-clé des plateformes en matière de détection

L'absence de projet de régulation internationale

Réguler les contenus nocifs : le consensus impossible ?

Le précédent du terrorisme

L'absence d'institutionnalisation internationale de la lutte contre la désinformation

Au-delà du consensus européen, des définitions confuses

Les limites des tentatives de régulation

L'absence d'approche commune du problème

Les contraintes du droit international

Des réponses difficiles à mettre en œuvre

Glossaire

Bibliographie sélective

Les auteurs

www.puf.com

1. Céline Marangé, désormais au Service historique de la Défense, était encore chercheuse à l'IRSEM (jusqu'au 30 juin 2020) lorsque le manuscrit du présent ouvrage a été remis.

1. Nicolas Mazzucchi, « L'économie, cible privilégiée de la guerre informationnelle ? », *Revue Défense Nationale*, mai 2014, n° 770, p. 22-27 ; François-Bernard Huyghe, Olivier Kempf et Nicolas Mazzucchi, *Gagner les cyberconflits*, Paris, Economica, 2015.

2. Le pouvoir discursif d'un État désigne la capacité pour un État à faire valoir son récit et ses vues politiques et à maîtriser les discours le concernant sur la scène internationale. Plus généralement, le pouvoir discursif peut se définir comme la « capacité des contributeurs aux espaces de communication à introduire, à amplifier et à maintenir des sujets, des cadres (de pensée) et des enceintes, façonnant ainsi les discours publics et les controverses qui se déploient dans des espaces de communication interconnectés » (Andreas Jungherr, Oliver Posegga, Jisun An, « Discursive power in contemporary media systems : A comparative framework », *The International Journal of Press/Politics*, 2019, vol. 24, n° 4, p. 404-425).

3. Carlo Muñoz, « Clapper calls for U.S. Information Agency "on steroids" to counter Russian propaganda », *The Washington Times*, 5 janvier 2017.

4. Sur la propagande totalitaire, voir Hannah Arendt, *Les Origines du totalitarisme*, t. 3 : *Le système totalitaire*, Paris, Seuil, 1995, p. 67-91.

5. Témoignage de Denise Abbey, *Foreign Affairs Oral History Project Information Series*, CD-Rom, Arlington, VA, ADST, 1998.

6. Robert Pirsein, *The Voice of America : An History of the International Broadcasting Activities of the United States Government : 1940-1962*, New York, Arno Press, 1979, p. 25-29.

7. Wilson P. Dizard, *Inventing Public Diplomacy. The Story of the U.S. Information Agency*, Londres, Lynne Rienner, 2004.

8. Nicholas Cull, *The Cold War and the United States Information Agency*, Cambridge, Cambridge University Press, 2008, p. 16-17.

9. Résolution du Politburo du Comité central du PCUS n° P81/8 sur « les missions des organes de sécurité dans la lutte contre les diversions idéologiques de l'adversaire », datée du 7 mai 1968 et signée par le chef du KGB Yuri Andropov, dans A. N. Âkovlev (dir.), *Lubânka. Organy VČK-OGPU-NKVD-MGB-MVD-KGB, 1917-1991* (*La Loubianka. Les organes de la Tchéka, de l'OGPU, du NKVD, du MGB, du MVD et du KGB, 1917-1991*), Moscou, Rosspen, 2003, en russe, p. 724-725.

10. Oleg Kalugin, *Prošaj, Lubânka !* (*Adieu, la Loubianka !*), Moscou, Olymp, 1995, en russe, p. 167-172.

11. Les illégaux étaient des Soviétiques infiltrés dans les pays occidentaux où ils dissimulaient leurs activités et leur origine.

12. *Kontrrazveditel'nyj slovar'* (*Dictionnaire de contre-espionnage*), Moscou, Département des éditions scientifiques de la Haute École du KGB Dzerjinski, 1972, en russe, p. 161-162.

13. Christopher Andrew, Vassili Mitrokhine, *Le KGB contre l'Ouest : 1917-1991*, Paris, Fayard, 2000, p. 334.

14. Maud Quessard, « Les combattants de la désinformation dans la nouvelle guerre froide », in *Stratégies d'influence et guerres de l'information*, Rennes, PUR, 2019, p. 107-121.

15. Alvin A. Snyder, *Warriors of Disinformation, American Propaganda, Soviet Lies and the Winning of the Cold War*, New York, Arcade Publishing, 1995.

16. Ladislav Bittman, *The New Image-Makers : Soviet Propaganda and Disinformation Today*, Washington, Pergamon-Brassey's, 1988, p. 18.

17. Alan K. Henrikson donne de la notion de « carte mentale » la définition suivante : « une structure de l'esprit par laquelle une personne acquiert, organise et stocke des représentations du monde qu'elle mobilise pour penser son action » (cité par Christian Lequesnes, *Ethnographie du Quai d'Orsay. Les pratiques des diplomates français*, Paris, CNRS Éditions, 2017, p. 156).

18. Thierry Balzacq, *Théories de la sécurité. Les approches critiques*, Paris, Presses de Sciences Po, 2016, p. 190-196.

19. Thierry Balzacq, Sarah Léonard, Jan Ruzicka, « "Securitization" revisited : Theory and cases », *International Relations*, 5 août 2015, vol. 30, n° 4, p. 494-531.

20. On distingue communément trois niveaux en stratégie. Le niveau opératif est celui où la campagne militaire interarmées est planifiée en fonction des buts de guerre et des orientations stratégiques, fixés par les dirigeants politiques. L'échelon tactique cible des objectifs locaux et vise à remporter une bataille sur le terrain d'opération.

21. Valeri Guerassimov, « Cennost' nauki v predvidenii » (« La valeur de la science est dans la prédiction »), *Voenno-promyshlennyj kur'er* (*Le Courrier militaro-industriel*), 27 février-5 mars 2013, vol. 8, n° 476, en russe. De larges extraits sont traduits dans Céline Marangé, *Les Stratégies et les Pratiques d'influence de la Russie*, Paris, IRSEM, *Études*, mars 2017, n° 49, p. 19-21.

22. Farhad Khosrokhavar, « Le cyber-califat de Daech », *Les Carnets du CAPS*, automne 2018, n° 26, p. 89-100.

23. Nicolas Chapuis, « "Digital China", ou comment la révolution numérique redistribue la puissance à l'échelle globale », *Les Carnets du CAPS*, automne 2018, n° 26, p. 75-88.

24. Voir Mathieu Duchâtel, François Godement, « L'Europe et la 5G : passons la cinquième » et « L'Europe et la 5G : le cas Huawei », *Notes de l'Institut Montaigne*, avril et mai 2019.

25. Frédérick Douzet, Alix Desforges, « Du cyberespace à la datasphère. Le nouveau front pionnier de la géographie », *Netcom*, 2018, n° 32-1/2, p. 87-108 ; Jean-Sylvestre Bergé, Stéphane Grumbach, « La sphère des données : objet du droit international et européen », *Journal du droit international*, septembre 2016.

26. Maud Quessard, Frédéric Heurtebize, Frédéric Gagnon (dir.), *Alliances and Power Politics in the Trump Era. America in Retreat ?*, Londres, Palgrave Macmillan, 2020.

27. Kevin Limonier, « Diffusion de l'information russe en Afrique. Essai de cartographie générale », IRSEM, 13 novembre 2018, note de recherche n° 66.

1. Sun Tzu, *L'Art de la guerre*, Paris, Flammarion, « Champs », 1972 : « Je fais en sorte que l'ennemi prenne mes points forts pour des points faibles […] j'observe le silence afin que nul ne puisse m'entendre » (p. 132) ; ou encore : « Ainsi avancez par des voies détournées et distrayez l'ennemi en l'appâtant […] Qui est capable d'agir ainsi comprend la stratégie du direct et de l'indirect » (p. 138-139), etc.

2. Azar Gat, *A History of Military Thought : From the Enlightenment to the Cold War*, Oxford, Oxford University Press, 2001.

3. Edward Bernays, neveu de Sigmund Freud dont il intègre certains travaux liés à la psychologie cognitive dans ses actions, a notamment fait partie de la Commission Creel (1917-1919) destinée à préparer la population américaine à l'entrée en guerre, puis de conduire une propagande en faveur de l'engagement dans les forces armées.

4. Élie Tenenbaum, *Partisans et centurions. Une histoire de la guerre irrégulière au XX^e siècle*, Paris, Perrin, 2018.

5. US DoD, *Principles of Strategic Communication*, août 2008.

6. Anthony H. Cordesman, *Iraq's Evolving Insurgency : The Nature of Attacks and Patterns and Cycles in the Conflict*, Washington, CSIS, 2006.

7. Allied Joint Publication 3.10 : Allied Joint Doctrine for Information Operations.

8. Charlie Winter, *The Virtual « Caliphate » : Understanding Islamic State's Propaganda Strategy*, Londres, Quiliam Foundation, 2015.

9. François-Bernard Huyghe, *Daech, l'arme de la communication dévoilée*, Paris, VA Press, 2017.

10. François-Bernard Huyghe, Olivier Kempf et Nicolas Mazzucchi, *Gagner les cyberconflits*, Paris, Economica, 2015.

11. Voir, entre autres, Rémy Hémez, *Opérations de déception. Repenser la ruse au XXI^e siècle*, Paris, IFRI, 2018.

12. Vincent Bernatis, « The Taliban and Twitter : Tactical reporting and strategic messaging », *Perspectives on Terrorism*, 2014, vol. 8, n° 6, p. 25-35.

13. Twitter dépasse les 200 millions de comptes actifs début 2013.

14. La page officielle du programme Scorpion de l'armée de terre est révélatrice de cette vision : https://www.defense.gouv.fr/terre/actu-terre/scorpion-sur-mesure-infocentre-et-infovalorise.

1. L'expression *Five Eyes* (« Cinq Yeux ») désigne l'alliance des services de renseignement de l'Australie, du Canada, de la Nouvelle-Zélande, du Royaume-Uni et des États-Unis.

2. Paul Baran, *On Distributed Communications : I. Introduction to Distributed Communications Networks*, Santa Monica, RAND Corporation, 1964.

3. On notera les travaux effectués à ce sujet par les chercheurs du centre GEODE (Paris), ainsi que par le Center for Applied Internet Data Analysis de l'université de San Diego. D'autres études existent, mais qui n'explicitent pas la portée géopolitique des routages.

4. Yves Lacoste, *La géographie, ça sert, d'abord, à faire la guerre*, Paris, La Découverte, « La Découverte Poche/Essais », 2014, édition augmentée, 249 p.

5. Paul Virilio, « Fin de l'histoire ou fin de la géographie ? Un monde surexposé », *Le Monde diplomatique*, août 1997.

6. John Allen, *Topologies of Power : Beyond Territory and Networks*, Londres, Routledge, 2016.

7. Mariannig Le Béchec, « Le territoire comme un graphe. Pratiques, formes, éthique », *Les Cahiers du numérique*, 2016, vol. 12, n° 4, p. 131-156.

8. John Law, *A Sociology of Monsters : Essays on Power, Technology and Domination*, Londres, Routledge, 1991.

9. Louis Petiniaud, Loqman Salamatian, *Geopolitics of Routing*, RIPE NCC, juillet 2019 ; voir https://labs.ripe.net/Members/louis_petiniaud/geopolitics-of-routing.

10. Théoriquement, les adresses IP sont géolocalisables. Or, les plages IP peuvent changer de propriétaire (et donc de localisation) d'autant plus rapidement qu'il existe désormais une pénurie mondiale d'IPV4 (les dernières adresses libres ont été allouées en octobre 2019). Voir James A. Muir et Paul C. van Oorschot, « Internet Geolocation : Evasion and Counterevasion », *ACM Comput. Surv.*, décembre 2009, vol. 42, n° 1, p. 4 : 1-4 : 23.

11. Nicole Starosielski, *The Undersea Network*, Durham, Duke University Press, 2015.

12. Kim Zetter, « Someone's been siphoning data through a huge security hole in the Internet », *Wired*, décembre 2013 ; voir https://www.wired.com/2013/12/bgp-hijacking-belarus-iceland/.

13. Dan Goodin, « BGP event sends European mobile traffic through China Telecom for 2 hours », *Ars Technica*, août 2019 ; voir https://arstechnica.com/information-technology/2019/06/bgp-mishap-sends-european-mobile-traffic-through-china-telecom-for-2-hours/.

14. Ksenia Ermoshina et Francesca Musiani, « Migrating servers, elusive users : Reconfigurations of the Russian Internet in the post-Snowden era », *Media and Communication*, 22 mars 2017, vol. 5, n° 1, p. 42.

15. En mars 2019, des courriers émis par le FSB à l'attention de plusieurs fournisseurs d'accès Internet russes ont été publiés, qui demandaient à ces acteurs de procéder à un « BGP

Blackhole » à l’encontre des serveurs du service mail chiffré suisse ProtonMail. Source : https://habr.com/en/company/tm/blog/443638/.

1. S’appuyant sur des procédés permettant de déterminer la localisation d’un émetteur d’ondes radioélectriques, la radiogoniométrie est notamment utilisée dans le cadre de la navigation aérienne ou maritime.

2. Chaque espace de confrontation (terre, air, mer, espace ou cyber) nécessite un très haut niveau de technicité, ce qui rend complexe le travail collaboratif entre armées, directions et services. Ainsi, un commandeur de forces terrestres aura du mal à prendre en compte les contraintes des forces liées aux autres milieux, maritime ou aérien par exemple, alors qu’il aura besoin d’elles pour réaliser ses missions.

1. Traduit de l'anglais par Maxime Chervaux.

2. Ashley May, « Photo of sad dad trying to sell donuts goes viral, and a sweet Twitter moment is born », *USA Today*, 12 mars 2019.

3. Jon Ronson, « How one stupid tweet blew up Justine Sacco's life », *The New York Times Magazine*, 12 février 2015.

4. Kaya Yurieff, « This nugget-loving kid just beat Ellen DeGeneres' retweet record », CNN, 9 mai 2017.

5. Tweet publié par Ellen DeGeneres le 2 mars 2014, consultable à l'adresse suivante : https://twitter.com/theellenshow/status/440322224407314432?lang=en.

6. Ben Nimmo, « #ElectionWatch : Alabama Twitter War », DFRLab, 17 novembre 2017. Voir https://medium.com/dfrlab/electionwatch-alabama-twitter-war-47b34ae89c50.

7. Ryan Broderick, « Meet the 29-year-old trying to become the king of Mexican fake news », BuzzFeed, 28 juin 2018.

8. Ben Nimmo, « #ElectionWatch : Alabama Twitter war », DFRLab, 30 juin 2018. Voir https://medium.com/dfrlab/electionwatch-hashtags-for-cash-in-mexico-1d2644a36412.

9. Samuel Woolley et Phil Howard, « Bots unite to automate the presidential election », *Wired*, 15 mai 2016.

10. David A. Broniatowski *et al.*, « Weaponized health communication : Twitter bots and Russian trolls amplify the vaccine debate », *American Journal of Public Health*, octobre 2018.

11. Nicholas Confessore *et al.*, « The follower factory », *The New York Times Magazine*, 27 janvier 2018.

12. Ben Nimmo et C. Shawn Eib, « Cross-platform spam network targeted Hong Kong protests », *Graphika*, 25 septembre 2019. Voir https://graphika.com/reports/spamouflage/.

13. Jason Skowronski, « Trolls and bots are disrupting social media – here's how AI can stop them », Towardsdatascience.com, 30 juillet 2019.

14. Lauren Papagalos, « Bots – The Good, The Bad And The Even Worse », sitelock.com, 31 mai 2016.

15. Yoel Roth, « Automation and the use of multiple accounts », Twitter, 21 février 2018. Voir https://blog.twitter.com/developer/en_us/topics/tips/2018/automation-and-the-use-of-multiple-accounts.html.

16. Ben Nimmo, « #BotSpot : Sex and sensibility », DFRLab, 3 juin 2018. Voir https://medium.com/dfrlab/botspot-sex-and-sensibility-dc1d4a72a92e.

17. Joseph Cox, « I bought a Russian bot army for under $100 », *The Daily Beast*, 13 septembre 2017.

18. *Idem.*

19. Facebook ne rend pas publique la date de création des comptes privés, mais on peut l'estimer en regardant la date de publication de la première photo de profil.

20. Ben Nimmo, « #ElectionWatch : Loves for sale in Brazil », DFRLab, 15 août 2018. Voir https://medium.com/dfrlab/electionwatch-loves-for-sale-in-brazil-f8033427dbe0.

21. Zi Chu, Steven Gianvecchio, Haining Wang et Sushil Jajodia, « Detecting automation of Twitter accounts : Are you a human, bot, or cyborg ? », *Dependable and Secure Computing*, IEEE Transactions on. 9. 811-824. 10.1109/TDSC.2012.75.

22. Yubao Zhang *et al*., « Twitter trends manipulation : A first look inside the security of Twitter trending », IEEE, 2016. Voir https://www.freeprojectsforall.com/wp-content/uploads/2017/10/Twitter-Trends-Manipulation-A-First-Look-Inside-the-Security-of-Twitter-Trending.pdf.

23. Ben Nimmo, « Le Pen's (small) online army », DFRLab, 6 mars 2017. Voir https://medium.com/dfrlab/le-pens-small-online-army-c754058630f0.

24. Ben Nimmo, « Measuring traffic manipulation on Twitter », Oxford Internet Institute, janvier 2019. Voir https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/01/Manipulating-Twitter-Traffic.pdf.

25. Ben Nimmo, « #ElectionWatch : Bots on both sides in India », DFRLab, 9 avril 2019. Voir https://medium.com/dfrlab/electionwatch-bots-on-both-sides-in-india-c87c84040229.

1. « Les photographes, en particulier les amateurs, vous diront que l'appareil ne peut pas mentir. Cela prouve simplement que les photographes, surtout les amateurs, le peuvent ; car la pellicule peut parfois tromper aussi bien que la toile. »

2. La science forensique regroupe l'ensemble des différentes méthodes d'analyse scientifiques servant au travail d'investigation.

3. Le *tracking* est une technique issue des effets spéciaux pour insérer des éléments artificiels dans une scène vidéo de façon cohérente avec les mouvements de l'image.

4. Hany Farid, *Photo forensics*, MIT Press, 2016.

5. Voir https://www.tineye.com.

6. Voir https://citizenevidence.amnestyusa.org.

7. Voir http://niessnerlab.org/projects/roessler2018faceforensics.html.

8. Voir https://deepfakedetectionchallenge.ai.

9. Rémi Géraud-Stewart, *Cyberspace and Time : A Light Through the Fog ?*, CIST, 2018 ; voir aussi le chapitre de Ben Nimmo dans cet ouvrage.

10. David Brin, « Self-addiction and self-righteousness », *in* Barbara Oakley, Ariel Knafo, Guruprasad Madhavan et David Sloan Wilson (éd.), *Pathological Altruism*, Oxford, Oxford University Press, 2011, chap. 5.

11. L'appareil photographique enregistre les coordonnées GPS au moment de la prise d'image.

12. Ainsi « APT28 », le profil derrière l'attaque de TV5 Monde et de nombreuses autres.

1. Kevin Limonier, *Ru.net : Géopolitique du cyberespace russophone*, Paris, L'Inventaire, 2008, p. 83-87.

2. Les structures de force (*silovye struktury*) désignent l'ensemble des organismes d'État pouvant faire usage de la force. Elles sont généralement chargées de l'application de la loi et dotées de pouvoir de surveillance et de répression.

3. Douglas Carman, « Translation and analysis of the doctrine of information security of the Russian Federation : Mass media and the politics of identity », *Pacific Rim Law & Policy Journal Association*, 2002, vol. 11, n° 2, p. 339-368.

4. « Doktrina informacionnoj bezopasnosti RF. Spravka. » (*Doctrine de sécurité de l'information de la Fédération de Russie. Information*), RIA Novosti, 9 septembre 2010, en russe ; voir https://ria.ru.

5. Doctrine de sécurité de l'information de la Fédération de Russie, adoptée par le décret présidentiel n° 646 du 5 décembre 2016 ; voir http://www.scrf.gov.ru.

6. Résolution du Politburo du Comité central du PCUS concernant la décision de créer au sein du KGB rattaché au Conseil des ministres de l'URSS une direction indépendante (la cinquième) pour l'organisation du travail de contre-espionnage dans la lutte contre les diversions idéologiques de l'adversaire », dans A. N. Âkovlev (dir.), *Lubânka. Organy VCK-OGPU-NKGB-MGB-MVB-KGB, 1917-1991* (*Loubianka. Les organes de la Tchéka, de la Guépéou, du NKGB-MGB-MVD-KGB, 1917-1991*), Moscou, Rosspen, 2003, en russe, p. 711-714.

7. Résolution du Politburo du Comité central du PCUS n° P81/8 sur « les missions des organes de sécurité dans la lutte contre les diversions idéologiques de l'adversaire », datée du 7 mai 1968 et signée par le président du KGB Youri Andropov, dans A. N. Âkovlev (dir.), *Lubânka. Organy…*, *op. cit.*, p. 724-725.

8. Doctrine de politique étrangère de la Fédération de Russie de 2008, adoptée par le décret présidentiel n° 646 du 5 décembre 2016 ; voir http://kremlin.ru.

9. Joseph S. Nye Jr., *Soft Power : The Means to Success in World Politics*, New York, PublicAffairs, 2004, p. 10.

10. Entretien de Sergueï Lavrov à *Rossiïskaïa Gazeta*, « Mâgkaâ sila » (« Soft power »), 30 octobre 2018, en russe.

11. Yulia Kiseleva, « Russia's Soft Power Discourse : Identity, Status and the Attraction of Power », *Politics*, 2015, vol. 35, n° 3-4, p. 316-329.

12. Le secrétaire général du Conseil de sécurité, Nikolaï Patrouchev, qui a dirigé le FSB de 1999 à 2008, définit en 2017 les révolutions de couleur comme un « instrument […] destiné à détruire l'État et le priver de sa souveraineté sous le prétexte d'une démocratisation ». Voir « Patrouchev : les tentatives d'organiser des révolutions de couleur en Russie sont vaines », *Rossijskaâ Gazeta*, 18 mai 2017, en russe.

13. Vladimir Poutine, « La Russie et le monde changeant », *Moskovskie Novosti*, 27 février 2012, en russe ; voir www.mn.ru.

14. Discours de Vladimir Poutine à la Conférence des ambassadeurs du 9 juillet 2012 ; voir www.kremlin.ru.

15. Doctrine de politique étrangère de la Fédération de Russie de 2013, adoptée par décret présidentiel le 12 février 2013, art. 20 ; voir http://www.mid.ru.

16. Doctrine de politique étrangère de la Fédération de Russie de 2016, adoptée par le décret présidentiel n° 640 du 30 novembre 2016, art. 3k ; voir http://kremlin.ru.

17. « Le chef de l'administration présidentielle Ivanov : une guerre de l'information a lieu contre Poutine et la Fédération de Russie », *RBK*, 23 octobre 2014, en russe.

18. Pour un historique complet du concept de « guerre de l'information », voir Jolanta Darczewska, « The anatomy of Russian information warfare : The Crimean operation, a case study », Center for Eastern Studies (Varsovie), *Point of View*, mai 2014, n° 42, p. 9-10.

19. Vladimir Novikov, « Ne pas tuer, mais subordonner », *Le Courrier militaro-industriel*, Vpk-news.ru, 16 décembre 2015, n° 48 (614), en russe ; voir http://vpk-news.ru/articles/28497.

20. Mark Galeotti, « I'm sorry for creating the "Gerasimov doctrine" », *Foreign Policy*, 5 mars 2018.

21. Valeri Guerassimov, « La valeur de la science est dans la prédiction », *Voenno-promyshlennyj kur'er* (*VPK. Le Courrier militaro-industriel*), 27 février-5 mars 2013, n° 8 (476), en russe ; traduit du russe par C. Marangé. Voir https://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf. Pour une analyse en anglais de cet article, voir le post de Mark Galeotti, intitulé « The "Gerasimov doctrine" and Russian non-linear war » sur son blog *In Moscow Shadows. Analysis and Assessment of Russian Crime and Security*, non daté.

22. Julien Nocetti, « La Russie en quête de son "Internet souverain" », *La Revue des médias*, 21 juin 2019.

23. Kevin Limonier, Colin Gérard, « Guerre hybride russe dans le cyberespace », *Hérodote*, 2017, n° 166-167, p. 152-153.

24. Maxime Audinet, « Comment RT et Sputnik tissent la toile de Moscou à l'étranger », *La Revue des médias*, 19 juin 2019 ; voir https://larevuedesmedias.ina.fr.

25. « Il n'y a aucune objectivité », *Kommersant*, 7 février 2012, en russe. Voir également l'article publié sur le site de RT le 16 août 2008, « War moves from battleground to broadcasting studio ».

26. Maxime Audinet, « Diplomaties publiques concurrentielles dans la crise ukrainienne : le cas de RT et Ukraine Today », *Revue d'études comparatives Est-Ouest*, 2018, vol. 2, n° 2, p. 171-204.

27. Kristin Roth-Ey, *Moscow Prime Time : How the Soviet Union Built the Media Empire That Lost the Cultural Cold War*, Londres, Cornell University Press, 2011.

28. Christopher Andrew, Vassili Mitrokhine, *Le KGB contre l'Ouest 1917-1991*, Paris, Fayard, 2000, p. 334.

29. Voir la partie consacrée à l'IRA dans le « rapport Mueller », « Russian "actives measures" social media campaigns », in *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, Special Counsel Robert R. Mueller III, mars 2019, vol. 1, p. 14-35.

30. Colin Gérard, « "Usines à trolls" russes : de l'association patriotique locale à l'entreprise globale », *La Revue des médias*, 21 juin 2019.

31. *Idem.* Voir également le rapport du Computational Propaganda Research Project, « The IRA, social media and political polarization in the United States, 2012-2018 », Université d'Oxford, 17 décembre 2018, 46 p.

32. Kevin Limonier, Colin Gérard, « Guerre hybride russe dans le cyberespace », art. cit., p. 148-149.

33. Jean-Baptiste Jeangène Vilmer, *The « Macron Leaks » Operation : A Post-Mortem*, Atlantic Council/IRSEM, 20 juin 2019.

34. Valeri Guerassimov, « La valeur de la science est dans la prédiction », art. cit.

35. Colonel Patrick Justel, « La guerre électronique, une question d'avenir », dans « Regards croisés sur la guerre électronique », IFRI, *Focus stratégique*, juillet 2019, n° 90, p. 21-22.

36. Margarita Konaev, Samel Bendett, « Russian AI-enabled combat : Coming to a city near you ? », *War on the Rocks*, 31 juillet 2019. Source d'origine : https://iz.ru/news/659503.

37. *Idem*.

38. Voir David J. Smith, « Russian cyber capabilities, policy, and practice », *Focus Quaterly*, hiver 2014.

1. Les « moyens détournés » sont ceux qui permettent de remporter un combat de manière indirecte, en évitant un affrontement direct en position d'infériorité.

2. La réflexion sur la guerre asymétrique est menée en Chine au sein du département d'études stratégiques de l'Académie des sciences militaires, qui a organisé plusieurs années de suite des colloques internationaux sur *L'Art de la guerre* de Sun Zi, ainsi qu'au sein de l'Université de défense nationale. L'ouvrage de référence sur la pensée stratégique chinoise contemporaine est Peng Guangqian, Yao Youzhi (dir.), *The Science of Military Strategy*, Pékin, Military Science Publishing House, 2005 (rééd. 2013).

3. Valérie Niquet, *Les Fondements de la stratégie chinoise*, Paris, Economica, 1997.

4. Valérie Niquet, *L'Art de la guerre de Sun Zi*, traduction et édition critique, Paris, Economica, 1988.

5. Voir notamment le 三十六计 (*Traité des 36 stratagèmes*), traduction française par François Kircher, Paris, Rocher, 2003.

6. Valérie Niquet, *L'Art de la guerre de Sun Zi*, *op. cit.*, « Des plans », article 1.

7. *Ibid.*, « De l'utilisation des espions », article 13.

8. Les organes d'agitation et de propagande – *otdel agitatsii i propagandi* – sont l'un des « apports » majeurs du léninisme. Le département de propagande a été immédiatement intégré au Parti communiste chinois dès sa création, en 1921, par les représentants du Komintern à Shanghai. Voir Nick Frisch, « The Bolsheviks in Beijing », *Foreign Affairs*, 18 octobre 2017 (https://www.foreignaffairs.com/articles/china/2017-10-18/bolsheviks-beijing).

9. Ainsi, pour Mao, la bombe atomique n'est qu'un « tigre de papier » face à la supériorité idéologique du peuple chinois. Cette affirmation est aussi une forme de « guerre de l'information », à destination interne et externe, faisant croire que l'on est puissant lorsqu'on est faible.

10. Mao Tsé-toung, *Intervention aux causeries sur la littérature et l'art*, Yenan, 1942.

11. Edgar Snow est l'auteur de *Red Star Over China*, 1937. Agnes Smedley a été la correspondante de plusieurs journaux occidentaux proches des forces communistes.

12. Valérie Niquet, *Les Relations sino-soviétiques pendant la Seconde Guerre mondiale*, thèse de troisième cycle, Paris 1 – Panthéon-Sorbonne, 1985.

13. *Idem*. L'Armée rouge prendra le nom d'Armée populaire de libération pendant la guerre civile contre les forces nationalistes à partir de 1945.

14. *Idem.*

15. 韬光养晦 : « Cachez votre brillant, prenez le temps ». Il s'agit d'un proverbe classique repris par Deng Xiaoping pour prôner la modestie et la patience stratégique tant que les capacités de la Chine ne lui donnent pas l'assurance de s'imposer.

16. Des applications couplées aux technologies de l'intelligence artificielle permettent de noter et distribuer des « bons » et « mauvais » points, en fonction de l'attitude conforme ou non de tout citoyen.

17. Shen Ximei, « The story of China's Great Firewall, the world's most sophisticated censorship system », 2 octobre 2019. Voir https://www.abacusnews.com/who-what/story-chinas-great-firewall-worlds-most-sophisticated-censorship-regime/article/3030478.

18. Joe Urchill, « Russia and China get a big win on Internet sovereignty », *Axios*, 21 novembre 2019.

19. « Les routes de la soie numériques, une projection extraterritoriale de la cyberdéfense chinoise ? », *Observatoire du monde cybernétique*, 3 juillet 2019. Voir https://omc.ceis.eu/les-routes-de-la-soie-numeriques-une-projection-extra-territoriale-de-la-cyberdefense-chinoise.

20. Rogier Creemers, « Le pivot de la cybergouvernance de la Chine », *Perspectives chinoises*, 2015/4. Voir https://journals.openedition.org/perspectiveschinoises/7205?file=1.

21. Nectar Gan, « Cyberspace controls set to strengthen under China's new Internet boss », *South China Morning Post*, 20 septembre 2018. Voir https://www.scmp.com/news/china/politics/article/2164923/cyberspace-controls-set-strengthen-under-chinas-new-internet.

22. New Zealand Ministry of Foreign Affairs and Trade, *Understanding China's Cybersecurity Law*, septembre 2017. Voir https://www.mfat.govt.nz/assets/China/Understanding-Chinas-cybersecurity-law.pdf.

23. Wang Baowen, « Liberation Army Daily » (13-20 juin 1995), *in* Michael Pillsbury, *Chinese Ways of Future Warfare*, Washington, National Defense University Press, 1997.

24. On peut citer par exemple l'OMS (Organisation mondiale de la santé), la FAO, l'Organisation de l'aviation civile internationale ou Interpol jusqu'à la disparition puis la condamnation pour corruption à Pékin de son directeur, ancien vice-ministre chinois de la Sécurité publique.

25. Anne-Marie Brady, *Marketing Dictatorship in Contemporary Chine*, Lanham, Rowman & Littlefield, 2008. Et Valérie Niquet, « "Confu-talk", the use of Confucian concepts in contemporary Chinese foreign policy », *in* Anne-Marie Brady (dir.), *China Thought Management*, Londres, Routledge, 2011.

26. Cette offensive a été particulièrement violente lors de la crise du Covid-19, avec la « diplomatie des masques » et l'activisme des représentations diplomatiques à l'étranger ou de porte-parole du ministère des Affaires étrangères à Pékin.

27. 新形势下强军的科学指南 (« Une boussole scientifique pour une armée puissante dans la nouvelle situation »), PLA General Political Department, 1er décembre 2014. Voir http://www.qstheory.cn/dukan/qs/2014-12/01/c_1113408713.htm.

28. *China's National Defense in 2004*. Voir http://en.people.cn/whitepaper/defense2004/defense2004.html.

29. *Idem*.

30. *Idem*.

31. Wang Baowen, « Liberation Army Daily » (13-20 juin 1995), *in* Michael Pillsbury, *Chinese Ways of Future Warfare*, *op. cit.*

32. Wang Pufeng, « The challenges of information warfare », *China Military Science*, 1995, *in* Michael Pillsbury (dir.), *Chinese Ways of Future Warfare*, *op. cit.*, et 战略学 (*The Science of Military Strategy*), Academy of Military Science, 2013. Voir https://fas.org/nuke/guide/china/sms-2013.pdf.

33. Florence Gaillard, Isabelle Facon, Isabelle Soubès-Vergès, Philippe Archilleas, *Sécuriser l'espace extra-atmosphérique*, rapport CSFRS-FRS, 2016.

34. J. R. Ng, « China broadens military options », *Asian Military Review*, 15 janvier 2020.

35. Wang Pufeng, « The challenges of information warfare », art. cit.

36. Voir https://flia.org/notice-state-council-issuing-new-generation-artificial-intelligence-development-plan.

37. J. R. Ng, « China broadens military options », art. cit.

38. Ministry of National Defense, the People's republic of China, *China Establishes Joint Logistic Support Force*, 13 septembre 2016. Voir http://eng.mod.gov.cn/TopNews/2016-09/13/content_4730336.htm. La Seconde artillerie (第二炮兵) était le nom des forces nucléaires et de missiles conventionnels et nucléaires de l'APL depuis sa création en 1966 jusqu'en 2015. Au mois de janvier 2015, le nom est devenu « force des lanceurs » (火箭军) à la suite d'une réforme institutionnelle de l'APL.

39. Department of Defense, *Annual Report to Congress. Military and Security Development Involving the PRC 2019*. PDF disponible à l'adresse suivante : https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019%20CHINA%20MILITARY%20POWER%20REPORT%20(1).PDF.

40. Deepak Sharma, « Integrated network electronic warfare, China concept of information war », *Journal of Defense Studies*, avril 2010, vol. 4, n° 2.

41. David E. Sanger, David Barboza, Nicole Perlroth, « Chinese army unit is seen as tied to hacking against US », *The New York Times*, 18 février 2013.

42. « China unveils Cyber Security Innovation Center », *Defense World.net*, 28 décembre 2017. Voir https://www.defenseworld.net/news/21644/China_Unveils_Cybersecurity_Innovation_Center#.XptgIlMza00.

43. « "Made in China 2025" plan unveiled to boost manufacturing », *Global Times*, 20 mai 2015. Voir https://gbtimes.com/made-china-2025-plan-unveiled-boost-manufacturing.

44. Voir http://chinainnovationfunding.eu/thousand-talents-plan.

1. 游凱翔 (You Kaixiang), « 國安局：中共對台灣同路媒體放消息帶風向 » (« Bureau de la sécurité nationale : le Parti communiste chinois diffuse des informations dans les médias taïwanais »), 中央通訊社 (Central News Agency), 2 mai 2019.

2. À la fin de la guerre civile en 1949, les troupes nationalistes de Chiang Kaï-shek ont trouvé refuge sur l'île de Taïwan, tandis que la Chine continentale tombait entre les mains des communistes. Depuis lors, la Chine essaie de mettre fin à l'indépendance *de facto* de Taïwan.

3. Timothy Cheek, *Propaganda and Culture in Mao's China*, Oxford, Clarendon Press, 1997 ; Anne-Marie Brady, *Marketing Dictatorship*, Lanham, Rowman & Littlefield, 2008.

4. Peter Mattis, « China's digital authoritarianism : surveillance, influence, and political control », *Hearing Before the House Permanent Select Committee on Intelligence*, Washington, 16 mai 2019.

5. La tactique du front uni est élaborée à l'origine par Lénine dans son essai *La Maladie infantile du communisme (le gauchisme)*, dans lequel il critique les communistes qui refusent, au nom de la pureté idéologique, d'exploiter les tribunes offertes par la vie démocratique en régime parlementaire.

6. 毛泽东 (Mao Zedong), « 共产党人 » (« Communistes »), 毛泽东选集 (*Anthologie des travaux de Mao Zedong*), octobre 1938.

7. Peter Mattis, « China's 'Three Warfares' in perspective », *War on the Rocks*, 30 janvier 2018.

8. Mark Stokes, Russell Hsiao, « The People's Liberation Army General Political Department : Political warfare with Chinese characteristics », *Project 2049 Institute*, 14 octobre 2013.

9. Chien-Jung Hsu, « China's influence on Taiwan's media », *Asian Survey*, mai-juin 2014, vol. 54, n° 3, p. 515-539.

10. J. Michael Cole, « Chinese Disinformation in Taiwan », *Taiwan Sentinel*, 30 décembre 2019.

11. Brian Hioe, « Fighting fake news and disinformation in Taiwan : An interview with Puma Shen », *New Bloom*, janvier 2020.

12. Voir par exemple : 羅承宗 (Luo Cheng-tsung), « 宗教組織無法管，中國吃定了台灣 » (« Taïwan ne peut contrôler ses temples, la Chine exploite cette faiblesse »), 思想坦克, (*Char de la pensée*), 5 novembre 2019.

13. Peter Pomerantsev, Michael Weiss, « The menace of unreality : How the Kremlin weaponizes information, culture and money », *The Interpreter*, 22 novembre 2014.

14. Jean-Baptiste Jeangène Vilmer, Paul Charon, « Russia as a hurricane, China as climate change : Different ways of information warfare », *War on the Rocks*, 21 janvier 2019.

15. Entretien avec J. Michael Cole, Taipei, janvier 2020.

1. Daniel Byman et Jennifer Lind, « Pyongyang's survival strategy: Tools of authoritarian control in North Korea », International Security, été 2010, vol. 35, n° 1, p. 44-74.

2. Jan Jin-sung, *Dear Leader*, Bruxelles, Ixelles Éditions, 2014.

3. Bradley K. Martin, *Under the Loving Care of the Fatherly Leader : North Korea and the Kim Dynasty*, New York, Thomas Dune Books, 2006.

4. La Corée du Sud a riposté en installant également des haut-parleurs diffusant musiques, chansons et messages politiques contre le Nord, de l'autre côté de la frontière.

5. Oscar Holland, « What North Korean propaganda poster reveal », CNN, 2 janvier 2018.

6. À Singapour en juin 2018, à Hanoï au Vietnam en février 2019, à la frontière entre les deux Corées dans la zone démilitarisée (Demilitarized Zone – DMZ) en septembre 2019.

7. Terrains de l'auteur en Corée du Nord, 25 septembre-4 octobre 2018 et 31 août-8 septembre 2019.

8. Korean Central News Agency. Voir www.kcna.kp.

9. Uriminzokirri, « Nous, parmi les nations ». Voir https://www.uriminzokkiri.com/index.php?lang=eng.

10. Le site North Korea Tech publie et met à jour un index documenté des principaux sites Internet nord-coréens. Il est tenu par un journaliste américain, Martyn Williams, qui assure un suivi des principales évolutions nord-coréennes en matière de technologie de l'information. Voir https://www.northkoreatech.org.

11. Stephan Haggard et Marcus Noland, *Famines in North Korea : Markets, Aid and Reform*, New York, Columbia University Press, 2007.

12. Anna Fifield, « A new film captures North Korea's "bold and audacious" millennials », *The Washington Post*, 15 décembre 2015 ; Jieun Back, *North Korea's Hidden Revolution : How the Information Underground Is Transforming a Close Society*, Yale University, 2016.

13. Naenara, « mon pays ». Voir http://naenara.com.kp/main/index/en/first.

14. Dave Lee, « North Korea : On the Net in world's most secretive nation », BBC News, 10 décembre 2012.

15. Martyn Williams, « North Korea's Koryolink : Built from surveillance and control », *38th North*, 26 juillet 2019. On notera l'appel à Huawei pour mettre en place un réseau crypté spécial destiné aux téléphones des cercles de pouvoir nord-coréens. Voir https://www.38north.org/2019/07/mwilliams072219/s.

16. Dave Lee, « North Korea : On the Net in world's most secretive nation », art. cit.

17. Terrains de l'auteur en Corée du Nord.

18. Nat Kretchun, « The regime strikes back : A new era of North Korean information controls », *38th North*, 9 juin 2017. Voir https://www.38north.org/2017/06/nkretchun060917.

19. Michael Raska, « Information warfare on the Korean Peninsula », *The Strategist*, 13 mars 2013 ; Kim Chong-woo, « The evolution of North Korean cyber threats », *Asan Institute for Policies Studies brief*, 20 février 2019.

20. Quentin Hodgson, Logan Ma, Krystyna Marcinek, Karen Schwindt, « Fighting shadows in the dark », rapport de la RAND, 2019 ; « 2019 midterm report UN panel of expert on North Korea », 30 août 2019, p. 23-30. Voir https://www.ncnk.org/sites/default/files/UN_POE_August2019.pdf.

21. Les États-Unis, suivis par des sociétés spécialisées en informatique comme Kaspersky et Symantec, ont accusé la Corée du Nord.

22. US Treasury Department, « Treasury sanctions North Korea state sponsored malicious cybergroups », 13 septembre 2019. Voir https://home.treasury.gov/news/press-releases/sm774.

23. Robert Potter, « Toward a better understanding of North Korea's cyber operations », *38th North*, 5 août 2019. Voir https://www.38north.org/2019/08/rpotter080519.

24. Jenny Jun, Scott Lafoy, Ethan Sohn, *North Korea's Cyber Operations : Strategy and Response*, CSIS, 30 décembre 2015.

25. Dagyum Ji, « ROK defense minister calls for "thorough" response to DPROK-linked hacking », *NKnews*, 12 octobre 2017.

26. Jenny Jun, Scott Lafoy, Ethan Sohn, *North Korea's Cyber Operations : Strategy and Response*, *op. cit.*

1. À l'instar du *ketman*, le *taqia* et *le khod'eh* sont de vieilles techniques de mystification intellectuelle cultivées par le clergé iranien pour assurer la survie et l'épanouissement de la cause chiite.

2. François Thual, *Géopolitique du chiisme*, Paris, Arléa, 2002, p. 45.

3. Shireen Hunter, « Iran's geopolitical predicament and its consequences », Loble Log, 7 mars 2017.

4. Christophe Réveillard, « L'Iran géopolitique », *Académie de géopolitique de Paris*, avril 2006.

5. Pierre Pahlavi, « Comprendre la résilience de la République islamique d'Iran », *Politique étrangère*, automne 2018, vol. 83, n° 3, p. 63-74.

6. Saeid Golkar, « The Islamic Republic's art of survival : Neutralizing domestic and foreign threats », Washington Institute for Near East Policy, », Policy Focus #125, juin 2013.

7. Sur l'impact de la guerre du Golfe : Hamid Mowlana, *Triumph of the Image : The Media's War in the Persian Gulf, a Global Perspective*, New York, Routledge, 2018.

8. G. Lucas, « State-sponsored Hacktivism and the Rise of "Soft" War », *Soft War*, 2017, p. 77-87.

9. Pierre Pahlavi, « Guerre irrégulière et analyse institutionnelle : le cas de la stratégie asymétrique des Gardiens de la révolution en Iran », *Études internationales*, 2011, vol. 42, n° 4, p. 485.

10. Michael Connell, « Iran's military doctrine », *The Iran Primer*, Washington, USIP Press Books, 2010, p. 71 ; Guy Freedman, « Iranian approach to deterrence : Theory and practice », *Comparative Strategy*, 2017, vol. 36, n° 5, p. 400-412.

11. Vahid Sepehri, « Iran : New commander takes over Revolutionary Guards », Radio Free Europe/Radio Liberty, 3 septembre 2007 ; Farhad Rezaei, « Iran and Israel : Taking on the "Zionist Enemy" », in *Iran's Foreign Policy after the Nuclear Agreement*, Londres, Palgrave Macmillan, 2019, p. 215-242.

12. Dan Dickerson, « Iran Would Strike First », *Journal of Counterterrorism & Homeland Security International*, 2010, vol. 16, n° 3, p. 31 ; J. Matthew McInnis, « Iran's strategic thinking : Origins and evolution », *AEI Paper & Studies*, 2015.

13. Nora Bensahel, « Darker shades of gray : Why gray zone conflicts will become more frequent and complex », *Foreign Policy Research Institute*, 2017.

14. Jason Rivera, « Understanding and countering Nation-State use of protracted unconventional warfare », *Small Wars Journal*, automne 2014.

15. James K. Wither, « Making sense of hybrid warfare », *Connections QJ15*, 2016, n° 2, p. 73-87.

16. F. Wehrey *et al.*, *The Rise of the Pasdaran : Assessing the Domestic Roles of Iran's Islamic Revolutionary Guards Corps*, RAND Corporation, vol. 821, 2009 ; Clément Therme, « Iran : la fin de la Révolution islamique ? », *Études*, mars 2018, n° 3, p. 19-30.

17. C. Sherrill, *Losing Legitimacy : The End of Khomeini's Charismatic Shadow and Regional Security*, Lanham, Rowman & Littlefield, 2018, p. 98.

18. « Iran's foreign minister attacks Twitter for allowing "pro-regime change bots" », SkyNews, 18 septembre 2018.

19. Muzammil Hussain, « The state of digital exception : Censorship and dissent in post-revolutionary Iran », in *State Power 2.0.*, Londres, Routledge, 2016, p. 47-58.

20. Sur l'exploitation des réseaux sociaux : Simin Kargar et Adrian Rauchfleisch, « State-aligned trolling in Iran and the double-edged affordances of Instagram », *New Media & Society*, 2019, vol. 21, n° 7, p. 1506-1527.

21. Walter Posch, « Ideology and strategy in the Middle East : The case of Iran », *Survival*, 2017, vol. 59, n° 5, p. 69-98.

22. Alexander Yonah et Milton Hoening, *The New Iranian Leadership : Terrorism, Nuclear Ambition, and the Middle East*, Westport, Praeger, 2008, p. 20.

23. S. Bradshaw et P. Howard, « The global organization of social media disinformation campaigns », *Journal of International Affairs*, 2018, n° 71, p. 23-32.

24. Michael Eisenstadt, « Iran's lengthening cyber shadow », *Washington Institute for Near East Policy*, juillet 2016, n° 34, p. 1-3.

25. Judith Palmer Harik, *Hezbollah : The Changing Face of Terrorism*, Londres, I.B. Tauris, 2006, p. 61 ; F. Rezaei, « Iran and Iraq : The lebanonization project in the balance », in *Iran's Foreign Policy after the Nuclear Agreement*, Londres, Palgrave Macmillan, 2019, p. 113-140.

26. James P. Terfry, *An Institutional Analysis of the Quds Force in Lebanon*, Canadian Forces College (Collège des Forces canadiennes), JCSP/PCEMI 39, avril 2013, p. 76-77 ; O. A. Honig et Ido Yahel, « The art of subversive conquest : How states take over sovereign territories without using military force », *Comparative Strategy*, 2017, vol. 36, n° 4, p. 293-308.

27. Cité dans M. Asser, « Hearts and minds : Hezbollah wages a propaganda war in the rubble of South Beirut », BBC, 18 août 2006.

28. Pierre Pahlavi, « The 33-day war : An example of psychological warfare in the information age », *Canadian Army Journal*, 2007, vol. 10, n° 2, p. 12-24 ; Emily Blout, « Iran's soft war with the West : History, myth, and nationalism in the new communications age », *SAIS Review of International Affairs*, 2015, vol. 35, n° 2, p. 33-44.

29. Pierre Pahlavi, « Understanding Iran's media diplomacy », *Israel Journal of Foreign Affairs*, 2012, vol. VI, n° 2, p. 21-33.

30. Sam Sasan Shoamanesh, « What of Iranian soft power ? », *GlobalBrief*, automne 2016, p. 34-36.

31. Alex Grinberg, « The concept of deterrence in Arab and Muslim thought – Iran », *Working Paper*, 13th Annual Herzliya Conference, 11-14 mars 2013. Pour un exemple, voir Mahdi

Javdani Moghaddam, « Rethinking on the backgrounds and roots of iranophobia discourse in international relations », *Islamic Political Thought*, 2019, vol. 5, n° 2, p. 107-126.

32. Sur le developpement de l'IRIB : Fardin Alikhah, « A brief history of the development of satellite channels in Iran », *Global Media and Communication*, 2018, vol. 14, n° 1, p. 3-29.

33. Iran, Iran French radio, « Qui sommes-nous ? », IRIB World Service. Voir http://french.irib.ir/accuiel/qui-sommes-nous (consulté en sept. 2019).

34. *Idem*.

35. Iran, Islamic Culture and Relations Organization. Voir en ligne : http://en.icro.ir/index.aspx?siteid=257&pageid=14454&p=1&showitem=361 (consulté en mars 2012).

36. Sam Sasan Shoamanesh, « What of Iranian soft power ? », art. cit., p. 36.

37. Iran, Payvand Iran News, « Ahmadinejad takes over Iranian official news agency », Payvand.com., 19 janvier 2011. Voir http://www.payvand.com/news/11/jan/1181.html (consulté le 25 nov. 2011).

38. C. A. Wege, « Iranian counterintelligence », *International Journal of Intelligence and CounterIntelligence*, 2019, vol. 32, n° 2, p. 272-294.

39. U.S. Government, *Iran's Ministry of Intelligence and Security : A Profile*, A Report Prepared by the Federal Research Division, Library of Congress under an Interagency Agreement with the Combating Terrorism Technical Support Office's Irregular Warfare Support Program, décembre 2012, p. 41-44.

40. À noter que l'armada satellite de l'Iran est en pleine expansion : Associated Press, « Iran state TV says country to launch 3 satellites this year – ABC News », 1er octobre 2019.

41. Iran, Press TV, Programs : voir https://www.presstv.com/Detail/2014/12/31/390988/About-PressTV (consulté en 2019) ; Abdol Moghset Bani Kamal, « Evaluating the Islamic Republic of Iran's public diplomacy », *Uluslararası Politik Araştırmalar Dergisi*, 2018, vol. 4, n° 2, p. 22-39.

42. Saeid Golkar, « The Islamic Republic's art of survival : Neutralizing domestic and foreign threats », art. cit., p. 15.

43. Abdol Moghset Bani Kamal, « Evaluating the Islamic Republic of Iran's public diplomacy », art. cit., p. 22-39.

44. Ramin Mostaghim et Borzou Daragahi, « Iran starts its own English satellite news », *Los Angeles Times*, juillet 2017.

45. Mark Sweney, « Iran's Press TV loses UK licence », *The Guardian*, 20 janvier 2012 ; Monroe Price, « Iran and the soft war », *International Journal of Communication*, 2012, n° 6, p. 19 ; Maysam Behravesh, « Press TV : Iran's revisionist voice in perspective », *Asian Politics & Policy*, 2013, vol. 5, n° 4, p. 683-686.

46. Hassan Dai, « Middle Eastern interventions in Africa : Tehran's extensive soft power », *Middle East Quarterly*, automne 2018, vol. 25, n° 4.

47. Penny L. Watson, « Iran's Latin America strategy : 2005 to present », *Democracy and Security*, 2017, vol. 13, n° 2, p. 127-143.

48. Clément Therme, « L'Iran en Amérique latine : entre romantisme révolutionnaire et intérêts stratégiques », *in* F. Nahavandi (dir.), *L'Iran dans le monde*, Paris, L'Harmattan, 2013, p. 218.

49. Michael Rubin, « Strategies underlying Iranian soft power », *American Enterprise Institute*, mars 2017.

50. Wazhmah Osman, « Between the White House and the Kremlin : A comparative analysis of Afghan and Tajik media », *International Journal of Communication*, 2019, n° 13, p. 23.

51. « Dar pai efsha saazi 8 Sobh, modakhela rasaana-yi Iran barasee meshawad », Hasht-e Sobh (Kabul), 14 août 2012.

52. Vera A. Achkasova, « Propaganda content in digital space : Identification markers », Communication Strategies in Digital Society Workshop (ComSDS), IEEE, 2019 ; Constance Duncombe, « Twitter and transformative diplomacy : Social media and Iran-US relations », *International Affairs*, 2017, vol. 93, n° 3, p. 545-562.

53. Majid KhosraviNik, « Macro and micro legitimation in discourse on Iran's nuclear programme : The case of Iranian national newspaper *Kayhan* », *Discourse & Society*, 2015, vol. 26, n° 1, p. 52-73.

54. U.S. Government, *Iran's Ministry of Intelligence and Security : A Profile*, *op. cit.*, p. 41.

55. Sur le développement de réseaux de « proxies » transnationaux : C. Clarke et P. Smyth, « The implications of Iran's expanding Shia foreign fighter network », *CTC Sentinel*, 2017, vol. 10, n° 10, p. 14-18.

56. Christopher Bing et Munsif Vengattil, « Facebook removes fake accounts tied to Iran that lured over 1 million followers », Reuters, 26 octobre 2018.

57. « Iranian hackers targeted Trump's re-election campaign », *The New York Times*, 4 octobre 2019.

58. « US worried by voter-influence efforts of Russia, China, Iran », ABC News, 19 octobre 2018.

59. Saeid Golkar, « The Islamic Republic's art of survival : Neutralizing domestic and foreign threats », art. cit., p. 15.

60. Michael Rubin, « Strategies underlying Iranian soft power », art. cit.

61. Jason Rivera, « Understanding and countering Nation-State use of protracted unconventional warfare », art. cit.

1. La fédération des Émirats arabes unis a acquis son indépendance le 2 décembre 1971. Elle est composée des émirats d'Abu Dhabi (capitale fédérale), de Dubaï (économie des services et tourisme), Sharjah (riche en gaz) et des émirats pauvres du Nord : Ajman, Umm al-Qaywayn, Ras al-Khaymah et Fujeyrah.

2. Le CCG est une organisation intergouvernementale créée lors du premier sommet constitutif à Abu Dhabi le 25 mai 1981. Elle comprend les six monarchies de la péninsule Arabique : Arabie saoudite, Bahreïn, Émirats arabes unis, Koweït, Oman et Qatar.

3. Il abdique le 25 juin 2013.

4. Hisham Sharabi, *Neopatriarchy : A Theory of Distorted Change in Arab Societies*, Oxford, Oxford University Press, 1992.

5. Michael Herb, *All in the Family : Absolutism, Revolution and Democracy in the Middle Eastern Monarchies*, Albany (NY), State University of New York Press, 1999.

6. Nous excluons les expatriés qui, bien que constituant souvent plus de la moitié de la population, voire plus de 85 % pour le Qatar et les EAU, ne bénéficient pas de la redistribution de la rente.

7. Pour une analyse détaillée, voir l'excellent ouvrage d'Andreas Krieg (éd.), *Divided Gulf. The Anatomy of a Crisis*, Londres, Palgrave Macmillan, 2019. Voir aussi pour la chronologie exhaustive de la crise : François Chauvancy, *Blocus du Qatar : l'offensive manquée. Guerre de l'information, jeux d'influence, affrontement économique*, Paris, Hermann Éditions, 2018.

8. À la demande du Qatar, les États-Unis ont dépêché une équipe du FBI pour enquêter et ont désigné les EAU comme le commanditaire de la cyberattaque survenue le 23 mai sur le site de la QNA, même si l'agence impliquée est russe et qu'Abu Dhabi a toujours démenti l'accusation. Voir Karen De Young, Elen Nakashima, « UAE orchestrated hacking of Qatari government sites, sparking regional upheaval, according to US intelligence officials », *The Washington Post*, 16 juillet 2017.

9. Andrew England, Ahmed Al Omran, « Saudi crown prince's inner circle vulnerable to shake-up », *Financial Times*, 12 décembre 2018.

10. Fatiha Dazi-Héni, *L'Arabie saoudite*, Paris, Tallandier, « En 100 questions », 2018, 2e éd.

11. Il est professeur de sciences politiques à University of United Arab Emirates, président du comité culturel de l'Association scientifique et culturelle de Dubaï et l'auteur de nombreux articles et ouvrages en relations internationales portant sur la sécurité du Golfe, dont *The Gulf Moment in Arab Contemporary History*, Beyrouth, Dar Al-Farabi, 2018.

12. Joseph Nye, « Power and Foreign policy », *Journal of Political Power*, 30 mars 2011, vol. 4, no 1, p. 9-24.

13. Au lendemain de la crise qui éclate le 5 juin, lorsque les pays du quartet décident de rompre leurs relations diplomatiques avec le Qatar, ils annoncent la fermeture de leur espace aérien et

maritime ainsi que de la seule frontière terrestre de la péninsule Arabique qui sépare le Qatar de son voisin saoudien d'où le Qatar importait l'essentiel de ses produits alimentaires et matériels de construction.

14. Fatiha Dazi-Héni, « La politique étrangère saoudienne », *Politique internationale*, novembre 2019, numéro hors-série « L'Arabie tentée par la réforme », p. 49-61.

15. Le wahhabisme est une variante saoudienne du salafisme, lecture fondamentaliste de l'islam sunnite.

16. Tom Lipman, « Qatar should commit to six principles », 5 juillet 2017 ; voir www.bh/portal/en/news/792679.

17. L'accord de Riyad du 23 novembre 2013 a été signé par le roi Abdallah d'Arabie saoudite, l'émir Tamim du Qatar et l'émir Sabah Al Ahmed Al Sabah du Koweït. Chacun des États du CCG s'engage à ne pas interférer dans les affaires des uns et des autres. L'accord interdit le financement des groupes dits « déviants » (radicaux, activistes anti-gouvernementaux) et stipule de ne pas soutenir les Frères musulmans et les opposants au gouvernement yéménite qui menacent les États du Golfe.

18. L'accord du 17 novembre 2014 met fin à une crise diplomatique qui a vu l'Arabie saoudite, les EAU et le Bahreïn rappeler leur ambassadeur du Qatar le 5 mars 2014, après que Doha a été accusé de ne pas avoir respecté les engagements de l'accord de Riyad, signé le 23 novembre 2013. La crise prend fin le 16 novembre avec la signature d'un accord qui correspond au retour des ambassadeurs.

19. Voir www.vision2030.gov.sa.

20. Eman Al Husein, « Saudi First : How hyper-nationalism is transforming Saudi Arabia », European Council of Foreign Relations, Policy Brief, 19 juin 2019. Voir www.ecfr.eu.

21. Fatiha Dazi-Héni, « Arabie saoudite : la nation selon Mohammed Bin Salman », *in* Olivier Da Lage (dir.), *L'Essor des nationalismes religieux*, Paris, Demopolis, 2018, chap. 4, p. 71-87.

22. Nous nous sommes rendue à plusieurs reprises en Arabie saoudite, entre 2017 et 2019, où nous avons réalisé de nombreux entretiens, portant notamment sur la crise, avec des officiels, des chercheurs et des jeunes.

23. Nicholas Cull, *Public Diplomacy : Lessons From the Past*, Los Angeles, Center on Public Diplomacy, Figueroa Press, 2009.

24. Mehrvan Kamravan, « The Foreign Policy of Qatar », *in* R. Hinnesbush, A. Eteshali (dir.), *The Foreign Policies of Middle East States*, Boulder (CO), Lynn Rienner Publishers, 2014, chap. 6, p. 157-183.

25. Le 27 juin 1995, le prince héritier cheikh Hamad Bin Khalifa Al Thani dépose son père l'émir Khalifa, alors en villégiature en Europe. Ce dernier était très lié à la famille royale Al Saoud et refusait d'exploiter le gisement gazier offshore. C'est alors que, soutenu par les États-Unis, le prince héritier s'empare du pouvoir. Ce n'est que sous la pression de Washington que Riyad reconnaît le nouvel émir.

26. Mehrvan Kamravan, « The Foreign Policy of Qatar », art. cit.

27. Le groupe se renforce et compte aujourd'hui, outre sa chaîne sportive beIN, deux sites Internet en arabe et en anglais, un centre d'études et de recherches et un centre de formation dans le domaine des médias. S'y ajoute le média en ligne et sur Twitter AJ+ depuis 2014 qui s'adresse essentiellement à une clientèle jeune et occidentale.

28. Dubaï World Port (DWP) est une société publique appartenant à l'émirat de Dubaï qui a acquis la compagnie maritime britannique Peninsula and Orient Steam et convoité, sans succès, de racheter en 2006 six ports américains.

29. James Mattis a été le secrétaire d'État à la Défense au sein de l'administration Trump du 20 janvier 2017 au 1er janvier 2019. Ce général quatre étoiles connaît parfaitement la région du Golfe pour avoir participé aux guerres du Golfe de 1991, d'Afghanistan et d'Irak et avoir commandé l'US Central Command.

30. Entretien avec un consultant de l'Emirate Diplomatic Academy (EDA), Abu Dhabi, octobre 2019.

31. Entretien avec une consultante, spécialiste des médias au NMC, Abu Dhabi, octobre 2019.

32. Giorgio Cafiero, « The "Trump factor" in the Gulf divide », *in* Andreas Krieg (éd.), *Divided Gulf. The Anatomy of a Crisis*, *op. cit.*, chap. 8, p. 127-144.

33. Yves Bourdillon, « Les discrètes affaires entre Israël et les monarchies du Golfe », *Les Échos*, 7 janvier 2020.

34. Ryan Grim, « Diplomatic underground : The sordid double life of a Washington's most powerful ambassador », 30 août 2017 ; voir www.theintercept.com.

35. Giorgio Cafiero, « Donald Trump : A win for the UAE ? », *Lobelog*, 28 novembre 2016.

36. Mark Hosenenball, « Trump Administration debates designating Muslim Brotherhood as terrorist group », Reuters, 9 janvier 2017.

37. Ben Freeman, *The Emiraty Lobby : How the UAE Wins in Washington*, Center for International Policy (CIP), Foreign Influence Transparency Initiative, octobre 2019. Le CIP est un organisme indépendant fondé en 1975 qui publie des rapports sur la politique étrangère américaine.

38. A. Krieg, « Never mind Russia, the UAE has united with AIPAC to capture Washington », *Middle East Eyes*, 9 mars 2018.

39. M. Mazzetti, D. Kirpatrick, « How 2 Gulf Monarchies sought to influence the White House », *The New York Times*, 21 mars 2018.

40. Hamad Al-Muftah, « Qatar's response to the crisis : Public diplomacy as a mean of crisis management », *in* Andreas Krieg (éd.), *Divided Gulf. The anatomy of a crisis*, *op. cit.*, chap. 14, p. 233-250.

41. Pour plus d'informations sur le sujet, voir François Chauvancy, *Blocus du Qatar : l'offensive manquée. Guerre de l'information, jeux d'influence, affrontement économique*, *op. cit*.

42. David D. Kirkpatick et Sheera Frenkel, « Hacking in Qatar highlights a shift toward espionage-for-hire », *The New York Times*, 8 juin 2017.

43. David D. Kirkpatick et Kenneth Vogel, « Indictment details how Emirates sought influence in 2016 campaign », *The New York Times*, 5 décembre 2019.

1. Chapitre traduit de l'anglais par Maxime Chervaux.

2. Ce chapitre reprend plusieurs conférences que j'ai données – au siège de l'OTAN, à Wilton Park, ainsi qu'à l'ISA San Francisco et à Toronto – sur la meilleure manière de répondre à la désinformation. J'ai observé au plus près certaines des activités décrites ici lorsque j'étais évaluateur extérieur de la diplomatie publique britannique dans les pays Baltes et les Balkans au Bureau des affaires étrangères et du Commonwealth [N.D.T. : FCO – Foreign Office, le ministère des Affaires étrangères britannique]. Je m'inspire également du travail réalisé grâce à une bourse d'études de l'école de journalisme de l'université d'Oxford au printemps 2019. Les opinions exprimées ici sont les miennes. Le résumé rédigé par Clare Feikert-Ahalt, pour la Bibliothèque du Congrès [https://www.loc.gov/law/help/fake-news/uk.php], est un bon point de départ pour s'imprégner des ressources qui fondent ce chapitre. Enfin, une bibliographie plus complète est disponible ici : https://citizenlab.ca/wp-content/uploads/2019/05/Disinformation-Bibliography.pdf.

3. Voir https://www.gov.uk/government/speeches/pm-speech-to-the-lord-mayors-banquet-2017.

4. Pour un rappel historique : A. Z. McKenna, *100 Years of Government Communication*, Londres, Cabinet Office, 2018, p. 11, en ligne ici : https://gcs.civilservice.gov.uk/wp-content/uploads/2018/09/100-years-of-Government-Communications-History.pdf ; pour Charles II, voir http://tei.it.ox.ac.uk/tcp/Texts-HTML/free/B02/B02127.html ; et pour Jacques II, voir http://tei.it.ox.ac.uk/tcp/Texts-HTML/free/A87/A87488.

5. Au sujet de la révolution américaine, voir Mark A. Genest, « The message heard round the word… », *in* Andrea Drew, Mark A. Genest et S. C. M. Paine (dir.), *From Quills to Tweets : How America Communicates About War and Revolution*, Washington DC, Georgetown University Press, 2019.

6. Voir Saul David, *The Indian Mutiny : 1857*, Londres, Penguin, p. 528 notamment.

7. Voir l'ouvrage classique portant sur la propagande durant la Grande Guerre : M. L. Saunders et Philip M. Taylor, *British Propaganda During the First World War, 1914-1918*, Londres, Macmillan, 1982.

8. Pour une analyse détaillée de ces évolutions, voir Philip M. Taylor, *The Projection of Britain : British Overseas Publicity and Propaganda, 1919-1939*, Cambridge, Cambridge University Press, 1981.

9. Voir Nicholas J. Cull, *Selling War : British Propaganda and American Neutrality in the Second World War*, New York, Oxford University Press, 1994.

10. Voir l'étude qui fait référence sur ce sujet : Sefton Delmer, *Black Boomerang : An Autobiography*, Londres, Secker & Warburg, 1962 ; et ce travail plus récent : Lee Richards, *Whispers of War : Underground Propaganda Rumour-Mongering in the Second World War*, Londres, PsyWar.org, 2010.

11. Sur l'inauguration du COI et du GIS, voir A. Z. McKenna, *100 Years of Government Communication*, *op. cit.*, chap. 4.

12. Alban Webb, *London Calling : Britain, The BBC World Service and the Cold War*, Londres, Bloomsbury, 2014, p. 57-58.

13. Pour un état des lieux du sujet, voir Rory Cormac, *Disrupt and Deny : Spies, Special Forces, and the Secret Pursuit of British Foreign Policy*, Oxford, Oxford University Press, 2018.

14. *Idem.* Et voir Rory Cormac, « Secrets and lies : Britain's dirty war in Ireland », *The Irish Times*, 17 mai 2018.

15. L'argument d'Armstrong, avancé devant la Cour suprême de la Nouvelle-Galles du Sud, recyclait alors une phrase utilisée par Edmund Burke et Mark Twain. Voir l'article « Economical with the truth » sur Wikipédia : https://en.wikipedia.org/wiki/Economical_with_the_truth.

16. Ces évolutions sont détaillées ici : Philip M. Taylor, *Munitions of the Mind : A History of Propaganda*, Manchester, Manchester University Press, 2003, 3e éd., p. 249-297.

17. Stephen Castle, « An everyday story of Russian working folk – starring Tony Blair », *Independent*, 5 octobre 1997.

18. Rhiannon Vickers, « Blair's Kosovo campaign : Political communications, the Kosovo War and the battle for public opinion », *Civil Wars*, printemps 2000, vol. 3, no 1, p. 54-70.

19. A. Z. McKenna, *100 Years of Government Communication*, *op. cit.*, chap. 8 ; pour la Chambre des lords, voir https://publications.parliament.uk/pa/ld200809/ldselect/ldcomuni/7/704.htm ; pour « l'affaire » Jo Moore, voir Stephen Byers, « Explained : the Jo Moore spin email row », *The Guardian*, 15 février 2002.

20. James Pamment, *British Public Diplomacy and Soft Power : Diplomatic Influence and the Digital Revolution*, Londres, Palgrave, 2016. L'approche par l'image de marque nationale (*nation branding*) étudie l'importance de la représentation d'une nation dans la tête des citoyens étrangers, cette représentation influençant leurs attitudes. Le *nation branding* cherche ainsi à développer cette représentation à l'avantage d'une nation. Voir Nicholas J. Cull, *Public Diplomacy : Foundations for Global Engagement in the Digital Age*, Cambridge, Polity, 2019, p. 120-140.

21. Luke Harding, « Sir John Chilcot delivers highly critical verdict on Iraq war but ex-PM says : "I believe we made the right decision" », *The Guardian*, 6 juillet 2016 ; voir en ligne : https://webarchive.nationalarchives.gov.uk/20160708115158 ; http://www.iraqinquiry.org.uk/media/246416/the-report-of-the-iraq-inquiry_executive-summary.pdf.

22. Voir en ligne : https://web.archive.org/web/20090121124913 ; http://security.homeoffice.gov.uk/news-publications/publication-search/general/Contest-Strategy?view=Binary.

23. Ian Cobain, Alice Ross, Rob Evans et Mona Mahmood, « Revealed : UK's covert propaganda bid to stop Muslims joining Isis », *The Guardian*, 2 mai 2016 ; Ian Cobain, Alice

Ross, Rob Evans et Mona Mahmood, « Inside Ricu, the shadowy propaganda unit inspired by the cold war », *The Guardian*, 2 mai 2016. Selon la théorie de la propagande, la propagande blanche couvre la persuasion politique provenant de sources clairement identifiées. La propagande noire couvre un effort de persuasion dont les sources sont délibérément trompeuses. La propagande grise couvre un effort de persuasion dont les origines sont peu claires. On retrouve des exemples pour chaque catégorie dans : Nicholas J. Cull, David Culbert et David Welch (dir.), *Propaganda and Mass Persuasion : A Historical Encyclopedia, 1500 to the present*, Santa Barbara, ABC-Clio, 2003, p. 41-42, p. 151-153 et p. 425-426.

24. Pour un résumé de la doctrine de l'OTAN à cette époque, voir en ligne : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/450521/20150223-AJP_3_10_1_PSYOPS_with_UK_Green_pages.pdf.

25. Pour l'utilisation britannique de la communication stratégique, voir James Pamment, « Strategic communication campaigns at the Foreign and Commonwealth Office : Managing mediatization during the Papal visit, the Royal Wedding, and the Queen's visit to Ireland », *International Journal of Strategic Communication*, 2015, vol. 9, n° 2, p. 118-133.

26. A. Z. McKenna, *100 Years of Government Communication*, *op. cit.*, chap. 9.

27. Paweł Surowiec et Philip Long, « Hybridity and soft power statecraft : The "GREAT" Campaign », *Diplomacy and Statecraft*, 2020, vol. 31, n° 1, p. 168-195.

28. Sur la création de la 77e brigade, voir « Army sets up new brigade "for information age" », BBC News, 31 janvier 2015. Voir https://www.bbc.com/news/uk-31070114.

29. Pour un exemple de cette représentation, voir le rapport *Portland Soft Power 30* qui place le Royaume-Uni à la première place de son classement en 2018 (p. 44) : https://softpower30.com/wp-content/uploads/2018/07/The-Soft-Power-30-Report-2018.pdf.

30. Nicholas J. Cull, *The Decline and Fall of the United States Information Agency : American Public Diplomacy, 1989–2001*, New York, Palgrave, 2012, p. 157.

31. « GCHQ to help tackle "dark Net" child abuse images », BBC News, 11 décembre 2014. Voir https://www.bbc.com/news/uk-30426164.

32. Luke Harding et Julian Borger, « "Now we really have a crisis" – Russia's man in London leaving the Foreign Office yesterday », *The Guardian*, 17 janvier 2008 ; Peter Finn, « British Unit is alleging "intimidation" by Moscow », *The Washington Post*, 18 janvier 2008. Un tribunal russe a finalement rejeté l'accusation de fraude fiscale et les activités du British Council ont pu reprendre dans le pays courant 2018.

33. Sur cette campagne de publicité, voir « From Russia with news », *Independent*, 15 janvier 2010 (https://www.independent.co.uk/news/media/tv-radio/from-russia-with-news-1869324.html).

34. Parmi les experts étrangers qui tirèrent la sonnette d'alarme, on retrouve Ron Diebert, du Citizen Lab de l'université de Toronto. Ces événements ont été admirablement détaillés par Peter Pomerantsev dans ses deux ouvrages : *Nothing Is True and Everything Is Possible : The Surreal Heart of the New Russia*, New York, PublicAffairs, 2014 ; et *This Is Not Propaganda : Adventures in the War Against Reality*, Londres, Faber & Faber, 2019.

35. La guerre hybride combine des activités cinétiques et médiatiques dans le but de tromper. Pour une introduction aux travaux sur la guerre hybride, depuis 2015, au sein de l'OTAN et de l'UE, voir http://www.natolibguides.info/hybridwarfare/home.

36. J'ai entendu cette expression de la bouche d'un directeur de la communication de l'OTAN en février 2014, durant une conférence de l'OTAN sur la diplomatie publique, et j'ai ensuite repris cette phrase dans mes propres remarques.

37. Voir https://democracyendowment.eu/en/news/551:bringing-plurality-balance-to-russian-language-media-final-recommendations.html.

38. Stephen Meister, « The "Lisa case" : Germany as a target of Russian disinformation », *Nato Review*, 25 juillet 2016.

39. Cette conceptualisation a été utilisée lors d'une conférence à Wilton Park (« Russian language media : Promoting plurality, balance and accessibility ») du 2 au 4 novembre 2016 (WP1493). Voir en ligne : https://www.wiltonpark.org.uk/wp-content/uploads/WP1493-Programme.pdf.

40. Le soutien de l'ambassade britannique est noté ici : https://www.stopfake.org/en/about-us.

41. Voir https://euvsdisinfo.eu.

42. Le rapport annuel de l'Atlantic Council pour 2017-2018 liste une contribution du FCO comprise entre 500 000 et 999 000 dollars, et le rapport annuel de 2018-2019 la porte au-delà de 1 million de dollars. Voir https://euagenda.eu/upload/publications/untitled-146348-ea.pdf ; et aussi : https://www.atlanticcouncil.org/wp-content/uploads/2019/09/Atlantic-Council-Annual-Report-2018%E2%80%932019.pdf. À propos du Digital Forensic Lab, voir https://www.digitalsherlocks.org/about.

43. Voir https://foreignpolicy.com/gt-essay/taking-on-the-kremlin-from-his-couch-eliot-higgins-bellingcat-russia.

44. Le soutien du FCO était public, mais il est devenu controversé en 2018. Il a ainsi été l'objet d'une question au Parlement européen : http://www.europarl.europa.eu/doceo/document/E-8-2019-000092_EN.html.

45. Le soutien du FCO est noté ici (p. 72) : *Annual Report & Accounts 2017/18, Year ended 31 March 2018*, BBC Media Action. Voir http://downloads.bbc.co.uk/mediaaction/annualreports/2017-2018.pdf.

46. « BBC News Serbian digital service goes live », BBC, 26 mars 2018. Voir en ligne : https://www.bbc.co.uk/mediacentre/latestnews/2018/bbc-news-serbian-digital-service-goes-live.

47. Sur ce programme de *Superheroes*, voir https://www.britishcouncil.ee/en/programmes/society/superheroes. Pour les documents budgétaires liés aux aspects *engage* et *enhance*, voir ces deux documents : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/787697/Counter_Disinformation_and_Media_Development_2018-2019.odt ; http://s3.amazonaws.com/thegovernmentsays-files/attachments/160/1601740-2-Counter_Disinformation_and_Media_Development_Programme.odt.

48. Voir https://publications.parliament.uk/pa/cm201719/cmselect/cmfaff/332/33202.htm.

49. Voir Ewen MacAskill, « Hostile states pose “fundamental threat” to Europe, says MI6 chief », *The Guardian*, 8 décembre 2016.

50. Voir https://www.gov.uk/government/speeches/pm-speech-to-the-lord-mayors-banquet-2017.

51. Pour plus de détails sur la stratégie du FCO, et pour une sélection de publications réunies par Corneliu Bjola, voir en ligne : http://www.cbjola.com/single-post/2019/03/08/The-%E2%80%98Dark-Side%E2%80%99-of-Digital-Diplomacy-Countering-Disinformation-and-Propaganda ; une enquête du *Guardian* est également intéressante dans ce cas : Luke Harding, « “Deny, distract and blame” : How Russia fights propaganda war », *The Guardian*, 3 mai 2018.

52. Voir « Spy poisoning : Russian diplomats expelled across US and Europe », BBC News, 26 mars 2018 ; « European nations top expel Putin’s diplomats », *The Times*, 24 mars 2018.

53. Voir notamment Alec Folwell, « UK’s response to Skripal poisoning was “proportionate”, according to UK opinion formers », *YouGov*, 14 juin 2018 ; et Matthew Smith, « Eurotrack : Europeans overwhelmingly suspect Russia was behind the Salisbury poisoning », *YouGov*, 3 avril 2018. Pour l’attitude des Russes, voir https://www.themoscowtimes.com/2018/10/25/only-3-percent-russians-believe-moscow-was-behind-skripal-attack-poll-says-a63297.

54. Https ://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/705347/6.4391_CO_National-Security-Review_web.pdf. Pour la doctrine Fusion et un diagramme explicatif, voir p. 10.

55. Voir la publication de Aiken datée du 12 juin 2018 : https://gcs.civilservice.gov.uk/disinformation.

56. Voir https://gcs.civilservice.gov.uk/news/alex-aiken-introduces-the-rapid-response-unit.

57. Voir https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf. Le rapport final a été dévoilé en février 2019 : https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf. Pour une description des problèmes liés à l’utilisation de *fake news*, voir Jennifer Kavanaugh et Michael D. Rich, *Truth Decay : An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life*, Santa Monica, RAND Corporation, 2018. En ligne : https://www.rand.org/pubs/research_reports/RR2314.html.

58. Plus de détails dans : Nicholas J. Cull, « Rough winds do shake the darling buds of May : Theresa May, British Public diplomacy and reputational security in the era of Brexit », *in* Pawel Surowiec et Ilan Manor (dir.), *Public Diplomacy and the Politics of Uncertainty*, New York, Palgrave, 2020.

59. Consulter le lien suivant : https://gcs.civilservice.gov.uk/wp-content/uploads/2019/08/6.5177_CO_RESIST-Disinformation-Toolkit_final-design_accessible-version.pdf.

60. Sur cette enquête, voir Andrew Roth et Jim Waterson, « Russian media regulator to investigate BBC’s operations », *The Guardian*, 21 décembre 2018 ; et *Ofcom Broadcast and on*

Demand Bulletin, Ofcom, 20 décembre 2018, n° 369 ; sur l'annonce de l'amende, consulter : https://www.ofcom.org.uk/about-ofcom/latest/media/media-releases/2019/ofcom-fines-rt.

61. Pour le piratage et la panique sur les blogs, voir notamment https://in-this-together.com/expose-network-and-the-open-information-partnership-part-1 ; https://21stcenturywire.com/2019/03/30/orwells-child-the-integrity-initiative-expands-creating-the-expose-network.

62. Pour la réponse du FCO, voir James Landale, « Russia-linked hack "bid to discredit" UK anti-disinformation campaign – Foreign Office », BBC News, 10 décembre 2018.

63. Pour une plus ample discussion du concept de sécurité réputationnelle, voir Nicholas J. Cull, *Public Diplomacy…*, *op. cit.*, p. 166-167.

64. Ce sujet est traité efficacement par James Ball, « When free societies copy Russian media tactics, there's only one winner », *The Guardian*, 9 janvier 2019.

65. Mary Dudziak, *Cold War Civil Rights : Race and the Image of American Democracy*, Princeton, Princeton University Press, 2000.

66. Vasily Gatov, « Research the revenge : What we're getting wrong about Russia Today », Open Democracy, 12 août 2018.

67. « Heaven has no rage like love to hatred turned », *in* William Congreve, *The Mourning Bride*, 1697.

68. Cette histoire a été rapportée dans Nicholas J. Cull, *The Cold War and the United States Information Agency : American Propaganda and Public Diplomacy, 1945-1989*, New York, Cambridge University Press, 2008, chap. 11.

69. Je développe cet argument plus en détail dans : Nicholas J. Cull, *Public Diplomacy…*, *op. cit.*, p. 166-170.

1. L'IRA établie à Saint-Pétersbourg a été inculpée par la justice américaine pour une campagne de *trolling* et de diffusion de fausses informations pendant la campagne de 2016.

2. Voir le *Rapport d'enquête sur l'ingérence de la Russie dans les élections présidentielles de 2016* du procureur spécial Robert Muller : US Department of Justice, *Report on the Investigation Into Russian Interference in the 2016 Presidential Election*, Washington DC, USGPO, mars 2019, vol. I. En ligne : https://www.justice.gov/storage/report.pdf.

3. Ellen Nakashima, « U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 Midterms », *The Washington Post*, 7 février 2019 ; Julian E. Barnes, « Cyber Command took down Russian troll farm for Midterms elections », *The New York Times*, 26 février 2019.

4. Le ministère de l'Intérieur (Department of Homeland Security, DHS), le ministère de la Justice, le département d'État (Department of State, DoS) et le FBI ont travaillé de concert sous le commandement du général Paul Nakasone. Nommé en mai 2018 par le ministre de la Défense James Mattis, il est alors directeur de la NSA et commandant du Cybercom, et dirige le Russia Small Group. Consulter le lien suivant : https://dod.defense.gov/News/Article/Article/1512994/cybercom-now-a-combatant-command-nakasone-replaces-rogers.

5. Julian E. Barnes, « U.S. begins first cyberoperation against Russia aimed at protecting elections », *The New York Times*, 23 octobre 2018.

6. DOD, *Consolidated Report Strategic communication and information operations*, Washington DC, US Congress, USGPO, mars 2010.

7. Senate Committee on Foreign Relations, « International cybersecurity strategy : Deterreing foreign threats and building global cyber norms », mai 2016, 114th Congress, 2nd session ; Senate Armed Service Committee, Joint Statement, James Clapper, Marcel Letter, Admiral Michael Rogers, « Foreign cyber threats to the US », 5 janvier 2017.

8. Les rapports de think tanks américains réalisés en réaction à la campagne de 2016, et aux « DNC Leaks », préconisent tous une approche « globale » de l'ensemble des acteurs institutionnels et de la société pour répondre aux menaces générées par l'utilisation malveillante des outils numériques contemporains (Daniel Fried, Alina Polyakova, « Democratic Defense Against Disinformation », Atlantic Council, février 2018).

9. Subcommitte on Emerging Threats and Capabilities of the Committee on Armed Services House of Representatives, « Crafting an information warfare and counter-propaganda strategy for the emerging security environment », Washington, USGPO, 15 mars 2017, 115th Congress, 1st session.

10. Department of Defense, « Information operations », Washington DC, Headquarters Department of the Army, août 1996, Field Manual n 100-6.

11. Elizabeth G. Troeder, « A whole-of-government approach to gray zone warfare », SSI, US Army War College, mai 2019.

12. Dans les milieux institutionnels américains, le cyberespace est souvent associé à l'usage d'Internet et perçu comme le moyen de diffuser largement et à moindre coût des messages politiques ; comme les nouvelles guerres de l'information se jouent largement sur Internet, la confusion entre cyberguerre et guerre de l'information est devenue un écueil récurrent pour les responsables opérationnels (Catherine A. Theohary, « Information warfare : Issues for Congress », Washington, National Security Policy, Cyber and Information Operations, CRS, 5 mars 2018).

13. National Defense Authorization Act (NDAAC) 2017. Voir en ligne : https://www.congress.gov/bill/114th-congress/senate-bill/2943/text.

14. L'exemple idoine de ces opérations de ciblage subversif sur le Homeland est devenu la campagne de 2016, comme le démontrent plusieurs études très documentées menées par les acteurs contemporains de la résilience. Voir les études et rapports réalisés par la société Graphika à New York : https://graphika.com.

15. La mission du BBG s'inscrit dans les stratégies d'engagement de la diplomatie américaine. L'ensemble du réseau ainsi constitué s'adresse à plus de 220 millions de personnes à travers le monde en cinquante-neuf langues, *via* les radios ondes courtes et moyennes, le satellite, Internet et les réseaux sociaux.

16. Voir l'interview de James Glassman, « James Glassman evaluates his tenure at State », *Public Diplomacy Magazine*, hiver 2009, p. 36-43. Voir http://publicdiplomacymagazine.com.

17. Voir l'analyse d'Anne-Marie Slaughter, « America's edge : Power in the Networked Century », *Foreign Affairs*, 2009, vol. 88, n° 1.

18. Le concept de *network state* (État-réseau), qui viendrait supplanter l'État-nation, permet de repenser les interactions entre les acteurs gouvernementaux et les acteurs privés (Manuel Castell, « The new public sphere : global civil society, communication networks, and global governance », *Annals Of The American Academy Of Social Sciences*, mars 2008, vol. 616, p. 78-89).

19. US Department of State, « 21st century statecraft ». Voir https://2009-2017.state.gov/statecraft/index.htm.

20. « Hillary Clinton milite pour la liberté sur Internet », *Le Monde*, 16 février 2011.

21. Eric Schmidt, Jared Cohen, *The New Digital Age : Reshaping the Future of People, Nations and Business*, New York, Alfred A. Knopf, 2013.

22. Department of Defense, « Information operations », *op. cit*.

23. Dans l'intervalle, après la guerre du Golfe, pour éviter les confusions sémantiques entretenues dans les milieux politiques, le Pentagone réserve le vocable de guerre psychologique exclusivement aux opérations menées par les forces spéciales américaines.

24. Les commandements américains interarmées régionaux ou « fonctionnels » sont répartis sur cinq continents et sont appelés COCOM (Centcom, Eucom, Africom, Indo-Pacom et l'USCybercom).

25. Wallin Matthew, « Military public diplomacy. How the military influence foreign audiences », *American Security Project*, White Paper, février 2015.

26. Mario Roscini, *Cyber Operations and the Use of Force in International Law*, New York, Oxford University Press, 2014, p. 12.

27. Tim Maurer, *Cyber Mercenaries. The State, Hackers, and Power*, Cambridge (NY), Cambridge University Press, 2018.

28. Gary D. Brown, Andrew O. Metcalf, « Easier said than done : Legal reviews of cyber weapons », *Journal of National Security Law & Policy*, 2014, n° 7, p. 116-118.

29. Office of the Director of National Intelligence, Remarks as delivered by The Honorable James R. Clapper Director of National Intelligence, « National intelligence, North Korea, and the national cyber discussion », International Conference on Cyber Security, Fordham University Wednesday, 7 janvier 2015.

30. Ces activités de soutien sont désignées par le sigle DSPD – Defense Support to Public Diplomacy (US DoD JP3-13).

31. Pour les définitions, voir Philip Seib, *Real-Time Diplomacy : Politics and Power in the Social Media Era*, New York, Palgrave, 2012.

32. Emma Louise Briant, *Propaganda and Counter-terrorism. Strategies for Global Change*, Manchester, Manchester University Press, 2015.

33. Le cas d'école pour les acteurs de terrain demeure l'attaque du site Web VOA News par l'armée cyber iranienne en 2011.

34. *End-goal* pour la doctrine américaine, ce qui confère un avantage comparatif au USOCOM (le commandement des forces spéciales américaines) sur les autres commandements militaires américains.

35. Matthew Armstrong, ex-gouverneur du BBG de l'administration Obama et membre honoraire du régiment des *Psy Ops* à Fort Bragg (Caroline du Nord). Voir https://warontherocks.com/2017/01/the-past-present-and-future-of-the-war-for-public-opinion.

36. Voir le récit de l'ex-sous-secrétaire d'État à la Diplomatie publique, Richard Stengel, *Information Wars. How We Lost the Global Battle Against Disinformation and What Can We Do About It*, New York, Grove Press, 2019.

37. Des menaces utilisées par une grande variété d'acteurs civils ou militaires, qui s'appuient sur des outils d'influence, parfois combinés, allant des médias sociaux aux cyberattaques de précision. Voir l'ouvrage de référence de Mary Kaldor, *New and Old Wars : Organised Violence in a Global Era*, New York, Polity Press, 2006, 2e éd.

38. David E. Sanger, *The Perfect Weapon, War, Sabotage and Fear in the Cyber Age*, New York, Penguin Random House, 2018.

39. Donald J. Trump Administration, « On offensive cyber operations », National Security Presidential Memoranda 13, 22 août 2019.

40. David E. Sanger et Nicole Perlroth, « U.S. escalates online attacks on Russia's power grid », *The New York Times*, 15 juin 2019.

41. Maj. Luke Karl, Maj. Joseph Lane et Cmdr. David Sanchez, « How to stop losing the information war », *Defense One*, 26 juillet 2018.

42. Ce commandement aurait pour vocation de remplacer le GEC et le CyberCom (Conrad Crane, « The United States needs an information warfare command : A historical examination », *War on the Rocks*, 14 juin 2019).

43. Christopher Paul, Colin P. Clarke, Michael Schwille, Jakub Hl.vka, Michael A. Brown, Steven Davenport, Isaac R. Porche III et Joel Harding, *Lessons From Others for Future U.S. Army Operations In and Through the Information Environment*, Santa Monica, RAND Corporation, 2018, RR-1925/1-A.

1. Sylvie Kauffman, « À Munich, les échos du chaos moyen-oriental », *Le Monde*, 19 février 2018.

2. Marc Semo, « À l'Assemblée générale de l'ONU, Netanyahou triomphant, Abbas sur la défensive », *Le Monde*, 28 septembre 2018.

3. Guillaume Gendron, « Nucléaire iranien : le show de Netanyahou laisse froid », *Libération*, 30 avril 2018.

4. Avishai Mandelblit, « Lawfare : The legal front of the IDF », *Military and Strategic Affairs*, avril 2012, vol. 4, n° 1. Avishai Mandelblit, conseiller spécial de Netanyahou, est aujourd'hui procureur général d'Israël.

5. La normalisation de l'État d'Israël désigne dans le vocabulaire politique israélien la reconnaissance de l'État d'Israël à l'international.

6. Gal Hadari, Asaf Turgeman, « Public diplomacy in army boots : The chronic failure of Israel's hasbara », *Israel Affairs*, 2018, vol. 24, n° 3, p. 482-499.

7. Sur l'histoire de la *hasbara*, voir Ron Schleifer, « Jewish and contemporary origins of Israeli hasbara », *Jewish Political Studies Review*, 2003, vol. 15, n° 1/2, p. 123-153 ; Giora Goodman, « Explaining the occupation : Israeli hasbara and the occupied territories in the aftermath of the June 1967 war », *Journal of Israeli History, Politics, Society, Culture*, 2017, vol. 36, n° 1.

8. Ron Schleifer, *Psychological Warfare in the Arab Israeli Conflict*, New York, Palgrave Macmillan, 2014.

9. Theodor Herzl, « Opening address at the First Zionist Congress », *in* Theodor Herzl, *Zionist Writings : Essays and Addresses*, New York, Herzl Press, 1973, vol. 1, p. 132-138.

10. Nahum Sokolow, « The Rathenaus : Father and son », *in* Nahum Sokolov (éd.), *Selected Writings : Personalities*, Jérusalem, The Zionist Library, 1958, p. 147-149.

11. Jonathan Cummings, *Israel's Public Diplomacy : The Problems of Hasbara, 1966-1975*, Lanham, Rowman & Littlefield, 2016.

12. Discours de Gideon Meir, site du ministère des Affaires étrangères israélien. Consulter en ligne : https://mfa.gov.il/mfa/abouttheministry/pages/what%20hasbara%20is%20really%20all%20about%20-%20may%202005.aspx.

13. Noam Chomsky, *Pirates and Emperors, Old and New : International Terrorism in the Real World*, Boston, South End Press, 2002, p. 182.

14. Edward Said, « Propaganda and War », *Media Monitors Networks*, 31 août 2011.

15. Noam Sheizaf, « Hasbara : Why does the world fail to understand us ? », *+972 Magazine*, 13 novembre 2011. Voir https://www.972mag.com/hasbara-why-does-the-world-fail-to-understand-us/27551.

16. Naomi Frye, « Eurovision's sanitized vision of Israel », *The New Yorker*, 21 mai 2019. Voir https://www.newyorker.com/culture/culture-desk/eurovisions-sanitized-vision-of-israel.

17. Daniella Peled, « Forget "Startup Nation," Israel's brand identity is occupation », *Haaretz*, 18 juillet 2013.

18. Voir par exemple le décret officiel « Octroi d'une aide pour la réalisation d'événements pro-israéliens sur le terrain », Ministère des Affaires stratégiques et de l'Information, 2015. Voir en ligne : https://www.gov.il/BlobFolder/generalpage/strategy/he/strategic_affairs.pdf.

19. Ron Schleifer, *Psychological warfare in the Arab Israeli conflict*, *op. cit*., p. 27-33.

20. Yossi Kuperwasser, David Siman-Tov (dir.), « The cognitive campaign : Strategic and intelligence perspectives », INSS, Memorandum n° 197, 2019.

21. Military Intelligence Directorate Website (https://www.idf.il/en/minisites/military-intelligence-directorate).

22. John Reed, « Unit 8200 : Israel's cyber spy agency », *Financial Times*, 10 juillet 2015.

23. David Sanger, *Confront and Conceal. Obama's Secret Wars and Surprising Use of American Power*, New York, Broadway Books, 2012.

24. « "Any Palestinian is exposed to monitoring by the Israeli Big Brother" », *The Guardian*, 12 septembre 2014.

25. Moshe Ya'alon, « The cognitive war as an element of national security : Based on personal experience », INSS, Memorandum n° 197, 2019.

26. Uri Friedman, « Israel Defense Forces live blogs Gaza offensive », *Foreign Policy*, 14 novembre 2012.

27. Human Rights Watch, « Precisely wrong. Gaza civilians killed by Israeli drone-launched missiles », 2019 (https://www.hrw.org/report/2009/06/30/precisely-wrong/gaza-civilians-killed-israeli-drone-launched-missiles).

28. Ronen Dangoor, « Consciousness As Leverage : The Israeli campaign regarding the Iranian nuclear program », INSS, Memorandum n° 197, 2019.

29. Yves Eudes, « Flame, un virus espion d'État », *Le Monde*, 20 juin 2012.

30. Discours du ministre Gilad Erdan au Deutscher Israelkongress, Francfort, 25 novembre 2018.

31. Stuart Winner, « Un nombre record de touristes ont visité Israël cette année, selon le ministère », *The Times of Israel*, 26 septembre 2019.

32. Benjamin Netanyahou, interview avec Matt Crouch, Trinity Broadcasting Network, 21 janvier 2020.

33. Anshel Pfeffer, « Israel is more focused on "hasbara" Than it is on policy », *Haaretz*, 2 mars 2012.

1. Nancy Snow, «Japan's Challenges in Public Diplomacy, An American Vision », Asie.Vision 81, Note de l'IFRI, 10 février 2016.

2. Marylène Gervais, « Soft power et diplomatie publique du Japon : Évolution et diversification de la politique d'influence japonaise », *in* Guibourg Delamotte, *Le Japon dans le monde*, Paris, CNRS Éditions, 2019.

3. *Diplomatic Bluebook 2019*, sur https://www.mofa.go.jp/fp/pp/page22e_000929.html.

4. « UN declined Abe's request to speak at Climate Summit », *Mainichi Shinbun*, 29 novembre 2019 sur https://mainichi.jp/english/articles/20191129/p2g/00m/0na/018000c.

5. « Que devrait être la diplomatie publique de l'avenir ? » (« これからの磁台におけるパブリ ックデイプロマシーはどうあるべきか ? »), Réunion du groupe d'information sur les aspects institutionnels des relations publiques et de la diplomatie culturelle (広報文化外交の制度的あり方に関する有識者懇談会). Voir http://www.mofa.go.jp.

6. *Diplomatic Bluebook 2019*, *op. cit*.

7. Voir https://www.cao.go.jp/en/pmf/pmf_11.pdf.

8. Valérie Niquet, *Le Japon. Un modèle en déclin ?*, Paris, Tallandier, « En 100 questions », 2019.

9. Nancy Snow, « Japan challenges in public diplomacy », art. cit.

10. Voir http://cj-fund.co.jp.

11. Nancy Snow, « Japan challenges in public diplomacy », art. cit.

12. Le choix du Brésil s'explique par la présence historique d'une forte communauté d'origine japonaise. Les États-Unis sont le principal allié du Japon depuis la guerre et le souvenir de relations diplomatiques anciennes, ainsi que leur statut commun de « plus proche allié des États-Unis », lient le Japon au Royaume-Uni.

13. En France, en dehors de quelques grandes villes, l'enseignement du japonais est inexistant. Certains enfants s'inscrivent au cours de chinois dans l'enseignement secondaire pour avoir accès au japonais par l'intermédiaire des *kanjis*.

14. Au mois de décembre 2019, un employé a pu vendre les données fiscales, *non cryptées*, des résidents de la préfecture de Kanagawa.

15. Le concept de *sharp power*, ou pouvoir de « manipulation », mais qui peut aussi se traduire par pouvoir « malin », est appliqué à la Russie et à la Chine.

1. Jean-Baptiste Jeangène Vilmer, Alexandre Escorcia, Marine Guillaume, Janaina Herrera, *Les Manipulations de l'information : un défi pour nos démocraties*, rapport du Centre d'analyse, de prévision et de stratégie (CAPS) du ministère de l'Europe et des Affaires étrangères et de l'Institut de recherche stratégique de l'École militaire (IRSEM) du ministère des Armées, Paris, août 2018.

2. Fabrice d'Almeida et Christian Delporte, *Histoire des médias en France, de la Grande Guerre à nos jours*, Paris, Flammarion, 2003.

3. Cette théorie, développée par l'universitaire américain Francis Fukuyama à la chute de l'URSS, postulait notamment l'universalisation de la démocratie libérale occidentale comme forme finale de tout gouvernement humain. Ce triomphe de la démocratie libérale signifiait dès lors la « fin de l'Histoire », c'est-à-dire le terme de l'évolution idéologique des sociétés. Voir Francis Fukuyama, *The End of History and the Last Man*, New York, Free Press, 1992.

4. L'action de Cambridge Analytica en amont du référendum sur le Brexit, qui en a profondément influencé les résultats, est un exemple de manipulation de l'information endogène, c'est-à-dire une déstabilisation menée au sein d'un État par un acteur national et non étranger.

5. Si les campagnes les plus médiatisées sont celles qui ont eu lieu aux États-Unis, au Royaume-Uni et en Allemagne, le Nigeria, le Kenya, le Soudan ou encore Taïwan n'ont pas été épargnés par ce phénomène.

6. Cette phase d'analyse a notamment été conduite sous l'égide de l'Institut de recherche stratégique de l'École militaire (IRSEM) et du Centre d'analyse, de prévision et de stratégie (CAPS).

7. Cette procédure n'est recevable que si les informations sont objectivement inexactes, diffusées massivement et de manière artificielle, et si elles conduisent à « troubler la paix publique ou la sincérité du scrutin » (https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000037847559&categorieLien=id).

8. À noter que cette crainte s'est également retrouvée au cœur des débats concernant la proposition de loi pour la lutte contre la haine sur Internet (« loi Avia »).

9. Le Code électoral, dans son article L52-1, interdit notamment « pendant les six mois précédant le premier jour du mois d'une élection et jusqu'à la date du tour de scrutin où celle-ci est acquise, l'utilisation à des fins de propagande électorale de tout procédé de publicité commerciale par la voie de la presse ou par tout moyen de communication audiovisuelle ». Cet article L52-1 du Code électoral est disponible à l'adresse suivante : www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000023883001&cidTexte=LEGITEXT000006070239&dateTexte=20110420.

10. Tels « Factuel »/« Fact Check » de l'AFP, « Les Décodeurs » du *Monde*, « Checknews » de *Libération*, ou encore « Vrai ou fake », qui réunit les services de l'ensemble de l'audiovisuel public.

11. On peut respectivement penser aux travaux de l'enseignante Rose-Marie Farinella avec ses élèves de primaire (http://www.ac-grenoble.fr/ien.cluses/spip.php?article678) ; à l'action d'associations comme Entre les lignes (http://entreleslignes.media/nos-actions/) ou Fake Off (https://www.fakeoff.fr/) ; au plan de développement de l'éducation aux médias et à l'information annoncé par Françoise Nyssen en 2018.

12. Voir https://eduscol.education.fr/cid133693/l-emi-et-le-programme-d-emc.html ; consulter également : https://eduscol.education.fr/cid95488/deconstruire-la-desinformation-et-les-theories-conspirationnistes.html

13. Andrew Guess, Jonathan Nagler, Joshua Tucker, « Less than you think : Prevalence and predictors of fake news dissemination on Facebook », *Science Advances*, 9 janvier 2019, vol. 5, n° 1. Voir https://advances.sciencemag.org/content/5/1/eaau4586.

14. Voir https://jti-rsf.org/fr/a-propos.

15. Voir https://disinfo.quaidorsay.fr.

1. Divina Frau-Meigs, *Faut-il avoir peur des « fake news » ?*, Paris, La Documentation française, 2019.

2. François-Bernard Huyghe, *Désinformation : les armes du faux*, Paris, Armand Colin, 2016 ; Antoine Violet-Surcouf (dir.), *Influence et réputation sur Internet : communautés, crises et stratégies*, Bailly, La Bourdonnaye, 2013.

3. HLEG, *A Multi-dimensional Approach to Disinformation*, Commission européenne, DG-Connect, 2018, p. 4.

4. Voir les rapports du Conseil de l'Europe, par Claire Wardle et Hossein Derakhsan, *Information Disorder : Toward an Interdisciplinary Framework for Research and Policy Making*, 2017 ; du ministère des Armées, CAPS/IRSEM, par Jean-Baptiste Jeangène Vilmer, Alexandre Escorcia, Marine Guillaume, Janaina Herrera, *Les Manipulations de l'information : un défi pour nos démocraties*, 2018 ; et de l'Institut Montaigne, *Media Polarization "à la française" ? Comparing the French and American Ecosystems*, 2019.

5. Jochai Benkler, Robert Faris et Hal Roberts, *Network Propaganda : Manipulation, Disinformation and Radicalization in American Politics*, Oxford, Oxford University Press, 2018.

6. Hunt Allcott et Matthew Gentzkow, « Social media and fake news in the 2016 election », *Journal of Economic Perspectives*, 2017, vol. 31, n° 2, p. 211-36. DOI : 10.1257/jep.31.2.211.

7. Andrew Guess, Brendan Nyhan, Jason Reifler, « Selective exposure to misinformation : Evidence from the consumption of fake news during the 2016 U.S. presidential campaign », janvier 2018. Voir http://www.dartmouth.edu/~nyhan/fake-news-2016.pdf.

8. Richard Fletcher, Alessio Cornia, Lucas Graves et Rasmus Kleis Nielsen, « Measuring the reach of "fake news" and online disinformation in Europe », Reuters Institute/University of Oxford, Factsheet, février 2018. Consulter en ligne : https://reutersinstitute.politics.ox.ac.uk/our-research/measuring-reach-fake-news-and-online-disinformation-europe.

9. Noé Gaumont, Maziyar Panahi, David Chavalarias, « Reconstruction of the socio-semantic dynamics of political activist Twitter networks – Method and application to the 2017 French presidential election », *PLoS ONE*, 19 septembre 2018, vol. 13, n° 9 (https://doi.org/10.1371/journal.pone.0201879) ; voir aussi David Chavalarias, Noé Gaumont, Maziyar Panahi, « Hostilité et prosélytisme des communautés politiques », *Réseaux*, 2019, n° 214-215(2), p. 67-107 (http://www.cairn.info/revue-reseaux-2019-2-page-67.htm).

10. Datapol. Voir https://politoscope.org/2017/11/datapol.

11. Institut Montaigne, *Media Polarization "à la française" ?…*, *op. cit.*, p. 5-7 ; voir aussi Ethan Zuckerman, « French media is polarizing but not the way we expected », *Columbia Journalism Review*, 2019 (https://www.cjr.org/politics/french-media-polarization.php).

12. Cette polarisation en ligne est aussi confirmée par Richard Fletcher, Alessio Cornia, Rasmus Kleis Nielsen, « How polarized are online and offline news audiences ? A comparative

analysis of twelve countries », *The International Journal of Press/Politics*, décembre 2019. Voir https://doi.org/10.1177/1940161219892768.

13. Commission européenne, « Plan d'action contre la désinformation », JOIN(2018) 36 final, note 11, p. 2. Voir https://eeas.europa.eu/sites/eeas/files/plan_daction_contre_la_desinformation.pdf.

14. Voir les résultats sur le site de la Stratcom : https://euvsdisinfo.eu.

15. Stratcom, « Internet trolling as a tool of hybrid warfare : The case of Latvia », 2017. Voir https://www.stratcomcoe.org/download/file/fid/3353.

16. Les travaux de Jonathan Albright confirment la même stratégie russe aux États-Unis, notamment *via* Instagram : « Instagram, meme seeding, and the truth about Facebook manipulation ». Voir https://medium.com/berkman-klein-center/instagram-meme-seeding-and-the-truth-about-facebook-manipulation-pt-1-dae4d0b61db5.

17. Stratcom, « Virtual Russian worlds in the Baltics : Russia's footprint in the Nordic-Baltic information environment », 2018, p. 5 et p. 8.

18. *Ibid.*, p. 5.

19. Eli Pariser, *The Filter Bubble : What the Internet Is Hiding From You*, Londres, Penguin Books, 2011.

20. Walter Quattrociocchi, Antonio Scala, Cass Sunstein, « Echo chambers on Facebook », Cambridge (MA), Harvard Law School, Discussion Paper n° 877. PDF téléchargeable à l'adresse suivante : http://www.law.harvard.edu/programs/olin_center/papers/pdf/Sunstein_877.pdf.

21. *Ibid.*, p. 14.

22. *Ibid.*, p. 11.

23. R. Kelly Garrett et Natalie Jomini Stroud, « Partisan paths to exposure diversity : Differences in pro- and counterattitudinal news consumption », *Journal of Communication*, août 2014, vol. 64, n° 4, p. 680-701 (https://doi.org/10.1111/jcom.12105) ; Frederik J. Zuiderveen Borgesius, Damian Trilling, Judith Möller, Balázs Bodó, Claes H. de Vreese, Natali Helberger, « Should we worry about filter bubbles ? », *Internet Policy Review*, 2016, vol. 5, n° 1 (https://policyreview.info/articles/analysis/should-we-worry-about-filter-bubbles).

24. Dan M. Kahan, « Ideology, motivated reasoning, and cognitive reflection », *Judgment and Decision Making*, juillet 2013, vol. 8, n° 4. Voir http://journal.sjdm.org/vol8.4.html.

25. Emilio Ferrara, Zeyao Yang, « Quantifying the effect of sentiment on information diffusion in social media », Ithaca, Cornell University, 19 juin 2015 ; arXiv : 1506.06072v1 [cs. SI].

26. Brian E. Weeks, « Emotions, partisanship, and misperceptions : How anger and anxiety moderate the effect of partisan bias on susceptibility to political misinformation », *Journal of Communication*, août 2015, vol. 65, n° 4, p. 699-719. Voir https://doi.org/10.1111/jcom.12164.

27. R. Kelly Garrett, « Facebook's problem is more complicated than fake news », *The Conversation*, novembre 2016. Voir https://theconversation.com/facebooks-problem-is-more-complicated-than-fake-news-68886.

28. Seth Flaxman, Sharad Goel, Justin M. Rao, « Filter bubbles, echo chambers, and online news consumption », *Public Opinion Quarterly*, 1er janvier 2016, vol. 80 (numéro spécial), p. 298-320. Voir en ligne : https://doi.org/10.1093/poq/nfw006.

29. Andrew Guess, Brendan Nyhan, Jason Reifler, « Selective exposure to misinformation… », art. cit., p. 11.

30. Eli Pariser, *The Filter Bubble…*, *op. cit.*, p. 50 sq.

31. David M. J. Lazer, Matthew A. Baum, Yochai Benkler, Adam J. Berinsky, Kelly M. Greenhill, Filippo Menczer, Miriam J. Metzger, Brendan Nyhan, Gordon Pennycook, David Rothschild, Michael Schudson, Steven A. Sloman, Cass R. Sunstein, Emily A. Thorson, Duncan J. Watts, Jonathan L. Zittrain, « The science of fake news », *Science*, 9 mars 2018, vol. 359, n° 6380, p. 1094-1096.

32. Soroush Vosoughi, Deb Roy, Sinan Arai, « The spread of true and false news online », *Science*, 9 mars 2018, vol. 359, n° 6380, p. 1146-1151.

33. Daniel Kahneman, *Système 1/Système 2. Les deux vitesses de la pensée*, Paris, Flammarion, 2012.

34. Stephan Lewandowsky, Ullrich Ecker, Colleen Seifert, Norbert Schwarz, John Cook, « Misinformation and its correction : Continued influence and successful debiasing », *Psychological Science in the Public Interest*, décembre 2012, vol. 13, n° 3, p. 106-131.

35. Divina Frau-Meigs, *Faut-il avoir peur des « fake news » ?*, *op. cit.*, p. 129-134.

36. Stephan Lewandowsky *et al.*, « Misinformation and its correction… », art. cit.

37. Walter Quattrociocchi, Antonio Scala, Cass Sunstein, « Echo chambers on Facebook », art. cit., p. 11-16.

38. « Déconstruire le conspirationnisme », conférence du 12 février 2015 avec la participation de Rudy Reichstadt, directeur de l'Observatoire du conspirationnisme (http://www.siglab.fr/fr/deconstruire-le-conspirationnisme.html) ; voir aussi Rudy Reichstadt, *L'Opium des imbéciles*, Paris, Grasset, 2019.

39. Myriam Revault d'Allonnes, *La Faiblesse du vrai. Ce que la post-vérité fait à notre monde commun*, Paris, Seuil, 2018 ; Stephan Lewandowsky, Ullrich Ecker, John Cook, « Beyond misinformation : Understanding and coping with the "post-truth" era », *Journal of Applied Research in Memory and Cognition*, 2017, vol. 6, n° 4 ; voir aussi Gérald Bronner, *La Démocratie des crédules*, Paris, Puf, 2013.

40. Hunt Allcott et Matthew Gentzkow, « Social media and fake news in the 2016 election », art. cit., p. 234-235.

41. Andrew Guess, Brendan Nyhan, Jason Reifler, « Selective exposure to misinformation… », art. cit., p. 14.

42. Rasmus Kleis Nielsen, Lucas Graves, « "News you don't believe" : Audience perspectives on fake news », Reuters Institute/University of Oxford, 2017. Voir https://reutersinstitute.politics.ox.ac.uk/our-research/news-you-dont-believe-audience-perspectives-fake-news.

43. Cambridge Analytica est une société britannique ayant récupéré sans leur consentement les données de 50 millions d'internautes américains *via* Facebook pour élaborer un logiciel permettant de prédire et d'influencer le vote des électeurs durant la campagne de 2016, en faveur de Donald Trump. *IRA vs United States* fait référence au procès qui a suivi la découverte de la ferme de trolls de Saint-Pétersbourg, l'Internet Research Agency (IRA), dont certains membres ont exporté des tactiques de désinformation russe en s'immisçant sur le territoire américain lors de la campagne de 2016.

44. Alexandre Serres, *Dans le labyrinthe*, Caen, C&F Éditions, 2012.

45. Pedro Domingos, Matt Richardson, « Mining the network value of customers », in *Proceedings of the Seventh ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, New York, 2001, p. 57-66 ; Pedro Domingos, Matt Richardson, « Mining knowledge-sharing sites for viral marketing », in *Proceedings of the Eighth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, New York, 2002, p. 61-70.

46. Sinan Aral et Dean Eckles, « Protecting elections from social media manipulation », *Science*, 30 août 2019, vol. 365, n° 6456, p. 858-861. DOI : 10.1126/science. aaw8243 ; voir aussi J. L. Kalla, D. E. Broockman, « The minimal persuasive effects of campaign contact in general elections : Evidence from 49 field experiments », *American Political Science Review*, 2018, n° 112, p. 148-166.

47. Divina Frau-Meigs et Sophie Jehel, *Les Écrans de la violence*, Paris, Economica, 1997.

1. Sur la qualification juridique en droit international des différentes menaces numériques pendant les élections présidentielles américaines de 2016 et françaises de 2017, voir François Delerue, *Cyber Operations and International Law*, Cambridge University Press, 2020, p. 245-257 ; Jens David Ohlin, « Did Russian cyber interference in the 2016 election violate international law ? », *Texas Law Review*, 2016, n° 95 ; Duncan B. Hollis, « Russia and the DNC hack : What future for a duty of non-intervention ? – Opinio Juris », *Opinio Juris*, 27 juillet 2016.

2. Hillary R. Clinton, United States Federal Bureau of Investigation (FBI). Voir https://vault.fbi.gov/hillary-r.-clinton.

3. Michael Riley et Jordan Robertson, « Russian hacks on U.S. voting system wider than previously known », *Bloomberg*, 13 juin 2017.

4. Brian Barrett, « America's electronic voting machines are sitting ducks », *Wired*, 2 août 2016 ; Lily Hay Newman, « Voting machines are still absurdly vulnerable to attacks », *Wired*, 28 septembre 2018.

5. Ellen Nakashima, « National intelligence director : Hackers have targeted 2016 presidential campaigns », *The Washington Post*, 18 mai 2016.

6. Sur l'attribution de ces cyberopérations, voir François Delerue, *Cyber Operations and International Law*, *op. cit.*, p. 66, p. 78-80, p. 89-91.

7. Susan Hennessey, « What does the US Government know about Russia and the DNC hack ? », *Lawfare*, 25 juillet 2016.

8. Thomas Rid, « All signs point to Russia being behind the DNC hack », *Motherboard*, 25 juillet 2016.

9. Search the DNC Email Database, WikiLeaks, 22 juillet 2016 (https://wikileaks.org/dnc-emails).

10. Ministère de la Justice de la Fédération de Russie, *Statement of Immunity of the Russian Federation Dated on 6 November 2018 on the Russian Federation's Immunity From the U.S. District Court's Jurisdiction Under the 1976 Foreign Sovereign Immunities Act and Other Issues Relating to the Democratic National Committee's Allegations in Case No. 1:18-CV-3501 (S.D.N.Y.)* [courriel], 6 novembre 2018.

11. Robert Muller, *Report on the Investigation Into Russian Interference in the 2016 Presidential Election*, États-Unis, Département de la Justice, avril 2019. Voir https://www.justice.gov/storage/report.pdf.

12. Julien Lausson, « Présidentielle : pourquoi François Hollande redoute des cyberattaques », *Numerama*, 15 février 2017.

13. Julien Lausson, « Cyberattaques : la France se dit prête à riposter en cas d'ingérence pendant la présidentielle », *Numerama*, 16 février 2017.

14. Vote électronique, Ministère de l'Europe et des Affaires étrangères. Voir www.diplomatie.gouv.fr/fr/services-aux-citoyens/droit-de-vote-et-elections-a-l-etranger/vote-electronique.

15. Camille Caldini, « Un compte caché aux Bahamas », Franceinfo, 4 mai 2017.

16. Jean-Baptiste Jeangène Vilmer, Alexandre Escorcia, Marine Guillaume, Janaina Herrera, *Les Manipulations de l'information*, rapport conjoint du CAPS (Centre d'analyse, de prévision et de stratégie du ministère de l'Europe et des Affaires étrangères) et de l'IRSEM (Institut de recherche stratégique de l'École militaire du ministère des Armées), 2018 ; Boris Toucas, « The Macron Leaks : The Defeat of Informational Warfare », Center for Strategic and International Studies, 2017 ; Jean-Baptiste Jeangène Vilmer, *The « Macron Leaks » Operation : A Post-Mortem*, Paris/Washington DC, IRSEM/Atlantic Council, 2019.

17. « EMLEAKS », *Pastebin*, 5 mai 2017 ; la page a été supprimée mais est toujours disponible en suivant ce lien : « EMLEAKS – Pastebin.com », *Archive. today*, 5 mai 2017.

18. Kevin Limonier et Louis Pétiniaud, « Cartographier le cyberespace », *Les Champs de Mars*, 2018, n° 30.

19. « Macron campaign emails », WikiLeaks, 31 juillet 2017. Voir https://wikileaks.org/macron-emails.

20. Voir notamment le rapport de la société de cybersécurité TrendMicro : Feike Hacquebord, « Two years of pawn storm : Examining an increasingly relevant threat », A Trend Micro Research Paper, 2017.

21. Martin Untersinger, « "MacronLeaks" : l'enquête pointe vers un piratage "simple et générique" », *Le Monde*, 2 juin 2017.

22. « Admiral Rogers says Intel community warned Russian hacking ahead Macron », C-SPAN, 9 mai 2017.

23. Original en anglais : « *[W]e succeeded, Trump is president. Unfortunately, Marine [Le Pen] did not become president. One thing worked, but not the other* » (Paul Moreira, « Guerre de l'info : au cœur de la machine russe », ARTE France, « Premières lignes », 2017).

24. Carole Cadwalladr, « AggregateIQ : the obscure Canadian tech firm and the Brexit data riddle », *The Guardian*, 31 mars 2018.

25. Les journaux *The Guardian* et *The Observer* ont publié une étude assez détaillée des activités de Cambridge Analytica et d'AggregateIQ : « The Cambridge Analytica Files », *The Guardian*, 2018. Voir https://www.theguardian.com/news/series/cambridge-analytica-files.

26. Mike Isaac, Sheera Frenkel et Kevin Roose, « Don't tilt scales against Trump, Facebook Executive warns », *The New York Times*, 7 janvier 2020. Voir https://www.nytimes.com/2020/01/07/technology/facebook-trump-2020.html.

27. Voir https://www.facebook.com/boz/posts/10111288357877121.

28. Defending Digital Democracy Project, « The state and local election cybersecurity playbook », Belfer Center for Science and International Affairs, Harvard Kennedy School, 2018.

29. David Ignatius, « The U.S. military is quietly launching efforts to deter Russian meddling », *The Washington Post*, 8 février 2019.

30. Voir https://www.legifrance.gouv.fr/eli/loi/2018/12/22/MICX1808387L/jo/texte.

31. Tom Burt, « Microsoft expands AccountGuard to 12 more countries in Europe », *Microsoft*, 20 février 2019 ; Microsoft, « Microsoft AccountGuard Program », février 2019.

1. Une étape intermédiaire a été franchie au début des années 2000 lorsque certains États, en premier lieu les États-Unis, ont dû revoir leur appareil de défense informationnelle pour contrer des attaques venant de groupes armés non étatiques, notamment al-Qaida.

2. La notion de « guerre hybride » a été introduite par le lieutenant-général James Mattis et le lieutenant-colonel Frank Hoffman en 2005 (« Future warfare : The rise of hybrid wars », *Proceedings Magazine*, U.S. Naval Institute, novembre 2005, vol. 131, n° 11). Elle peut être définie comme « le mélange d'activités coercitives et subversives, de méthodes conventionnelles et non conventionnelles (c'est-à-dire diplomatiques, militaires, économiques, technologiques), susceptibles d'être utilisées de façon coordonnée par des acteurs étatiques ou non étatiques en vue d'atteindre certains objectifs, sans que le seuil d'une guerre déclarée officiellement ne soit dépassé » (Commission européenne, *Cadre commun en matière de lutte contre les menaces hybrides*, Bruxelles, 6 avril 2016).

3. « *Information Defense* » est le terme revendiqué par Ben Nimmo, comme l'indiquait son titre lorsqu'il était au Digital Forensic Research Lab (DFRLab) de l'Atlantic Council (« Senior Fellow for Information Defense »). Depuis 2019, il est « Director of Investigations » chez Graphika.

4. Ce chapitre s'appuie notamment sur Jean-Baptiste Jeangène Vilmer, Alexandre Escorcia, Marine Guillaume, Janaina Herrera, *Les Manipulations de l'information : un défi pour nos démocraties*, rapport du Centre d'analyse, de prévision et de stratégie (CAPS) du ministère de l'Europe et des Affaires étrangères et de l'Institut de recherche stratégique de l'École militaire (IRSEM) du ministère des Armées, Paris, août 2018 ; et sur Jean-Baptiste Jeangène Vilmer, *The « Macron Leaks » Operation : A Post-Mortem*, Paris/Washington DC, IRSEM/Atlantic Council, 2019.

5. Le design organisationnel est traditionnellement défini comme le « processus de décision visant à assurer une cohérence entre les buts ou objectifs pour lesquels l'organisation existe, les schémas de division du travail et de coordination entre unités et les personnes qui effectueront le travail » (Jay R. Galbraith, *Organization Design*, Reading (MA), Addison-Wesley Pub. Co., 1977, p. 5).

6. Cette association fréquente ne doit pas conduire à confondre les deux dans la mesure où l'objectif d'une attaque dite « hybride » est de générer de l'ambiguïté (si elle est bien conduite, la cible met du temps à comprendre qu'elle est attaquée et par qui), tandis que l'attaque terroriste est le plus souvent revendiquée : son objectif n'est pas d'entraver l'attribution, mais au contraire de la permettre et de l'assumer. Cela ne veut pas dire qu'en pratique un service associant les deux fera la confusion, puisqu'il peut réunir des équipes travaillant en parallèle. Dans le cas tchèque, le fait de préciser que le centre lutte contre « le terrorisme *et* les menaces hybrides » implique bien une différenciation, même si, par commodité organisationnelle sans doute, les deux sont réunis.

7. Entretien avec un responsable singapourien, Singapour, 5 novembre 2019.

8. US Senate, *Putin's Asymmetric Assault on Democracy in Russia and Europe : Implications for U.S. National Security*, A Minority Staff Report Prepared for the Use of the Committee on Foreign Relations, 10 janvier 2018, 115th Congress, Second Session (https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf).

9. UK House of Commons, Digital, Culture, Media and Sport Committee, *Disinformation and « Fake News » : Final Report*, 14 février 2019. PDF téléchargeable à l'adresse suivante : https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf.

10. Parliament of Australia, « Foreign interference through social media ». Voir en ligne : https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Foreign_Interference_through_Social_Media/ForeignInterference.

11. Singapore, *Report of the Select Committee on Deliberate Online Falsehoods*. PDF en ligne : https://www.rajahtannasia.com/media/pdf/Exec_Summary_Rpt_on_Deliberate_Online_Falsehoods.pdf.

12. Voir par exemple « Singapore "falsehoods" law shows perils of fake news fight », *Financial Times*, 3 février 2020.

13. En février 2020, l'agence suédoise des contingences civiles (MSB) en avait déjà formé 13 000 (entretien au MSB, le 5 février 2020).

14. En France, le Secrétariat général de la défense et de la sécurité nationale (SGDSN) les avait alertés dès la fin de l'été 2016 et, en octobre, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) – qui dépend du SGDSN – a organisé pour eux un séminaire sur la cybersécurité (Jean-Baptiste Jeangène Vilmer, *The « Macron Leaks » Operation : A Post-Mortem*, *op. cit.*, p. 31-32).

15. Comme l'a fait la Belgique avec Stopfakenews.be.

16. Le MSB a envoyé par la poste près de 5 millions d'exemplaires d'une brochure expliquant quoi faire en cas de crise, qu'il s'agisse d'une attaque terroriste ou d'une manipulation de l'information. Voir https://www.dinsakerhet.se/siteassets/dinsakerhet.se/broschyren-om-krisen-eller-kriget-kommer/om-krisen-eller-kriget-kommer---engelska.pdf.

17. Dès 2017, l'Italie a ajouté l'objectif de pouvoir « reconnaître les fake news » aux programmes scolaires ; plusieurs États américains, dont la Californie et le Massachusetts, ont adopté des lois en ce sens en 2018 ; tandis que depuis juillet de la même année la Suède développe les « compétences numériques » dans ses écoles, etc.

18. Le plan canadien révélé en janvier 2019 prévoit ainsi 7 millions de dollars pour des projets permettant de sensibiliser la population au risque que présente la désinformation en ligne.

19. La Russie est à la 149e place (sur 180) dans le classement de Reporters sans frontières. Voir https://rsf.org/fr/classement.

20. Une alliance des services de renseignement des États-Unis, du Royaume-Uni, du Canada, de l'Australie et de la Nouvelle-Zélande.

21. Jean-Baptiste Jeangène Vilmer, *The « Macron Leaks » Operation : A Post-Mortem*, *op. cit.*, p. 30.

22. Cité *supra*, p. 365.

23. 2016/2276(INI) – 15/06/2017. *Text adopted by Parliament, single reading*.

24. Représentation en France de la Commission européenne, « Code de bonnes pratiques contre la désinformation, un an après : les plateformes en ligne soumettent leurs rapports d'autoévaluation », 29 octobre 2019 (https://ec.europa.eu/france/news/20101029/rapport_code_bonne_conduite_desinformation_fr).

25. « Une Europe qui protège : l'UE fait rapport sur les progrès réalisés dans la lutte contre la désinformation en vue du Conseil européen », communiqué de presse du 14 juin 2019. Voir en ligne https://ec.europa.eu/commission/presscorner/detail/fr/IP_19_2914.

26. Élodie Lamer, « Vera Jourova, vice-présidente de la Commission européenne : "Le temps des accords avec les géants du Net est révolu" » (interview de Vera Jourova, vice-présidente de la Commission européenne pour les valeurs et la transparence), *Le Soir*, 10 février 2020.

27. Ce que les opérations chinoises à Taïwan et Hong Kong semblent confirmer : sur cette réduction de l'écart Russie-Chine, voir Jean-Baptiste Jeangène Vilmer et Paul Charon, « Russia as a hurricane, China as climate change : Different ways of information warfare », *War on the Rocks*, 21 janvier 2020.

28. Peter Pomerantsev et Michael Weiss, *The Menace of Unreality : How the Kremlin Weaponizes Information, Culture and Money*, New York, The Interpreter/Institute of Modern Russia, 2014.

29. Christophe Deloire, cité dans François Bougon, « Un label pour redonner confiance dans le journalisme », *Le Monde*, 3 avril 2018.

30. Ben Nimmo, « Investigative standards for analyzing information operations », à paraître.

31. Le *takedown* est une procédure par laquelle les plateformes suppriment des contenus illicites ou contrevenant à leurs règles (dans le cas de Facebook, par exemple, cette procédure vise des pages ou des comptes ayant un « comportement inauthentique coordonné »).

32. Voir dans ce volume le chapitre de Divina Frau-Meigs.

33. Jean-Baptiste Jeangène Vilmer, *The « Macron Leaks » Operation : A Post-Mortem*, *op. cit.*, p. 39-40.

34. Jean-Baptiste Jeangène Vilmer *et al.*, *Les Manipulations de l'information…*, *op. cit.*, p. 173.

35. Shelby Grossman, Daniel Bush et Renée DiResta, « Evidence of Russia-linked influence operations in Africa », Working Paper, Freeman Spogli Institute for International Studies, Stanford University, 29 octobre 2019. En octobre 2019, Facebook a également supprimé trois réseaux de comptes ayant un « comportement inauthentique coordonné », attribués à des acteurs russes visant des pays africains. Voir https://about.fb.com/news/2019/10/removing-more-coordinated-inauthentic-behavior-from-russia.

36. Voir aussi les recommandations de James Pamment, The EU's Role in Fighting Disinformation: Taking Back the Initiative, Carnegie Endowment for International Peace, 15 juillet 2020.

37. Dan Fried et Alina Polyakova, *Democratic Defense Against Disinformation*, Atlantic Council, 5 mars 2018 ; Jean-Baptiste Jeangène Vilmer, *The « Macron Leaks » Operation : A Post-Mortem*, *op. cit*., p. 46.

38. Ben Nimmo, Camille François, C. Shawn Eib, L. Tamora, « From Russia with blogs », Graphika, 12 février 2020.

39. L'attribution, qui consiste à déterminer qui est à l'origine d'une opération cyber, est notoirement difficile, voire impossible dans de nombreux cas, compte tenu de la complexité d'identifier le système informatique utilisé. Et, quand bien même remonterait-on jusqu'à un ordinateur, cela ne dirait pas qui se trouve derrière et si cette personne agit de sa propre initiative ou sous le contrôle d'un État. Sur la manière dont Facebook traite les difficultés de l'attribution, voir Alex Stamos, « How much can companies know about who's behind cyber threats ? », Fb.com, 31 juillet 2018.

1. Voir Ulf Häussler, « Cyber security and defence from the perspective of articles 4 and 5 of the NATO Treaty », *in* Anna-Maria Tallihärm (éd.), *International Cyber Security Legal & Policy Proceedings*, NATO CCDCOE, 2010.

2. *NATO Policy on Cyber Defence*.

3. Voir Mathhijs Veenendaal, Kadri Kaska, Pascal Brangetto, « Is NATO ready to cross the Rubicon on cyber defence ? », NATO CCDCOE, 2016 ; consulter https://ccdcoe.org/uploads/2018/10/NATO-CCD-COE-policy-paper.pdf.

4. Philippe Leymarie, « “Mort cérébrale” : l’OTAN bouge-t-elle encore ? » (https://blog.mondediplo.net/mort-cerebrale-l-otan-bouge-t-elle-encore).

5. Point 72 de la déclaration. Voir https://www.nato.int/cps/fr/natohq/official_texts_112964.htm.

6. Suivant la définition française, une cyberattaque est une « action volontaire, offensive ou malveillante, menée au travers du cyberespace et destinée à provoquer un dommage (en disponibilité, intégrité ou confidentialité) aux données ou aux systèmes qui les traitent, pouvant ainsi nuire aux activités dont ils sont le support ».

7. Michael Schmitt (dir.), *The Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge, Cambridge University Press, 2013 ; Michael Schmitt et Liis Vihul (dir.), *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge, Cambridge University Press, 2017.

8. Engagement en faveur de la cyberdéfense. Voir sur le site Web de l’OTAN : www.nato.int/cps/en/natohq/official_texts_133177.htm?selectedLocale=fr.

9. Voir Kenneth Geers, *Cyber War in Perspective : Russian Aggression Against Ukraine*, Tallinn, NATO CCDCOE, 2015.

10. Voir Matthijs Veenendaal et Pascal Brangetto, « Influence cyber operations : The use of cyberattacks in support of influence operations », in *8th International Conference on Cyber Conflict Proceedings*, NATO CCDCOE, 2016.

11. « Nous reconnaissons le cyberespace en tant que domaine d’opérations dans lequel l’OTAN doit se défendre aussi efficacement qu’elle le fait dans les airs, sur terre et en mer » (point 70 du communiqué du sommet de Varsovie qui s’est tenu les 8 et 9 juillet 2016).

12. Sur les exercices *Locked Shields* et *Crossed Swords*, voir le site du NATO CCDOE à Tallinn : www.ccdcoe.org.

13. Voir Fred Kaplan, « Inside “Eligible Receiver” » (https://slate.com/technology/2016/03/inside-the-nsas-shockingly-successful-simulated-hack-of-the-u-s-military.html).

1. Yochai Benkler, Robert Faris, Hal Roberts, *Network Propaganda, Manipulation, Disinformation and Radicalization in American Politics*, Oxford, Oxford University Press, 2018, p. 268.

2. Camille François, « Actors, behaviors, content : A disinformation ABC. Highlighting three vectors of viral deception to guide industry & regulatory responses », Working Paper of the Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression, 20 septembre 2019.

3. Maison Blanche, « Statement by the President on actions in response to Russian malicious cyber activity and harassment », 29 décembre 2016.

4. François Delerue, *Cyber Operations and International Law*, Cambridge, Cambridge University Press, 2020, p. 238-256 ; Nicholas Tsagourias, « Electoral cyber interference, self-determination and the principle of non-intervention in cyberspace », EJIL : Talk !, 26 août 2019.

5. Kevin Limonier, « Diffusion de l'information russe en Afrique. Essai de cartographie générale », IRSEM, 13 novembre 2018, Note de recherche n° 66, 21 p.

6. Clint Watts, « Advanced persistent manipulators », 12 février 2019. Consulter en ligne : https://securingdemocracy.gmfus.org/advanced-persistent-manipulators-part-one-the-threat-to-the-social-media-industry.

7. Frédérick Douzet, « Le cyberespace, troisième front de la lutte contre Daech », *Hérodote*, 2016, n° 160, p. 223-238.

8. Twitter, « Information operations directed at Hong Kong », 19 août 2019.

9. Camille François, « Actors, behaviors, content : A disinformation ABC. Highlighting three vectors of viral deception to guide industry & regulatory responses », art. cit.

10. Facebook, « Coordinated inauthentic behavior explained », 6 décembre 2018.

11. Google, « How Google fights disinformation », 9 février 2019.

12. Facebook a notamment partagé des informations sur les contenus et comptes supprimés dans le cadre de l'initiative *Coordinated and Inauthentic Behavior*.

13. California Senate Bill 1001. Consulter le site California Legislative Information : https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1001.

14. Camille François, « Actors, behaviors, content : A disinformation ABC. Highlighting three vectors of viral deception to guide industry & regulatory responses », art. cit.

15. *Joint Declaration on Freedom of Expression and « Fake News », Disinformation and Propaganda*, 3 mars 2017, FOM. GAL/3/17.

16. A/69/723 (9 janvier 2015) ; A/C.3/72/12 (11 octobre 2017).

17. S/RES/2129(2013), § 14 (17 décembre 2013).

18. S/RES/2354(2017), § 4 (e) (24 mai 2017).

19. S/2017/375, annexe « Cadre international global de lutte contre la propagande terroriste » (28 avril 2017).

20. *Ibid*., p. 6, § 14. De même, la *Stratégie antiterroriste mondiale* de l'Organisation des Nations unies recommande l'élaboration de ces partenariats : A/RES/60/288, annexe « Plan d'action », § 13 (8 septembre 2006).

21. Voir notamment A/RES/60/288, annexe « Plan d'action », § 13 (8 septembre 2006) ; G7, Réunion des ministres de l'Intérieur, communiqué de presse « La lutte contre l'emploi d'Internet à des fins terroristes et d'extrémisme violent », 5 avril 2019.

22. Le lien entre terrorisme et extrémisme violent a été établi par le Conseil de sécurité des Nations unies dans sa résolution 2178 (2014) adoptée le 24 septembre 2014.

23. *Appel de Christchurch pour supprimer les contenus terroristes et extrémistes violents en ligne*, 15 mai 2019, préambule.

24. Sur la notion d'action informationnelle, voir Colin Gérard, Kevin Limonier, « Guerre hybride russe dans le cyberespace », *Hérodote*, 2017, n° 166-167, p. 145-163.

25. Jean-Baptiste Jeangène Vilmer, Alexandre Escorcia, Marine Guillaume, Janaina Herrera, *Les Manipulations de l'information* : un défi pour nos démocraties, rapport du Centre d'analyse, de prévision et de stratégie (CAPS) du ministère de l'Europe et des Affaires étrangères et de l'Institut de recherche stratégique de l'École militaire (IRSEM) du ministère des Armées, Paris, août 2018, p. 132-138.

26. Commission européenne, « Consultation publique sur les fausses nouvelles et la désinformation en ligne », 13 novembre 2017.

27. Commission européenne, « Call for applications for the selection of members of the High Level group on fake news », 12 novembre 2017.

28. Commission européenne, *Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions. Lutter contre la désinformation en ligne : une approche européenne*, 26 avril 2018, COM(2018) 236 final.

29. Peter H. Chase, « The EU code of practice on disinformation : The difficulty of regulating a nebulous problem », *Working Paper of the Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression*, 29 août 2019.

30. Cela n'empêche toutefois pas l'Union européenne d'avoir adopté plusieurs règlements et directives permettant d'encadrer partiellement ces comportements et créant des obligations pour les plateformes.

31. Claire Wardle, Hossein Derakhsan, *Information Disorder : Toward an interdisciplinary Framework for Research and Policy Making*, Council of Europe Report, DGI(2017)09, 2017, 107 p. ; Edson C. Tandoc Jr. (éd.), « Defining "fake news" », *Digital Journalism*, 2018, vol. 6, n° 2, p. 137-153.

32. Emmanuel Macron a ainsi qualifié RT et Sputnik d'organes de propagande en mai 2017 lors d'une conférence de presse commune avec Vladimir Poutine : « Vidéo : regardez la conférence de presse commune entre Vladimir Poutine et Emmanuel Macron en intégralité », Franceinfo, 29 mai 2017.

33. A/RES/74/27, § 2 (27 décembre 2019).

34. GA/SHC/4284 (18 novembre 2019).

35. Loi organique n° 2018-1201 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information ; loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information. Le Conseil constitutionnel a précisé la notion dans sa décision du 20 décembre 2018 : Conseil constitutionnel, décision n° 2018-773 DC du 20 décembre 2018 « Loi relative à la lutte contre la manipulation de l'information », § 21 et § 23.

36. Pacte international relatif aux droits civils et politiques, adopté le 16 décembre 1966, ouvert à la signature le 19 décembre 1966, entré en vigueur le 23 mars 1976, article 19 (3). Voir également Comité des droits de l'homme, *Observation générale 34 « Article 19 : Liberté d'opinion et d'expression »*, 12 septembre 2011, CCPR/C/GC/34.

37. Voir notamment C.E.D.H., *Lopuch c. Pologne* (jugement), 24 juillet 2012, n° 43587/09 ; C.E.D.H., *Ahmet Yildrim c. Turquie* (arrêt), 18 décembre 2012, n° 3111/10 ; C.E.D.H., *Schuman c. Pologne* (décision), 3 juin 2014, n° 52517/13 ; C.E.D.H, *Delfi AS c. Estonie* (arrêt), 16 juin 2015, n° 64569/09.

38. Voir notamment « Vœux du président de la République Emmanuel Macron à la presse », 3 janvier 2018 ; « Discours du président de la République, Emmanuel Macron, lors du forum sur la gouvernance de l'Internet à l'UNESCO », 12 novembre 2018.

39. Tel est notamment le cas dans la loi française sur les manipulations de l'information, le juge des référés pouvant ordonner le retrait de contenus aux plateformes (article L. 163-2-II du Code électoral).

40. Twitter a finalement autorisé la diffusion des publicités encourageant la participation électorale (https://twitter.com/twitterfrance/status/1113702072887545857).

This file was downloaded from Z-Library project

Your gateway to knowledge and culture. Accessible for everyone.

z-library.sk z-lib.gs z-lib.fm go-to-library.sk

Official Telegram channel

Z-Access

https://wikipedia.org/wiki/Z-Library